

CIS Red Hat Enterprise Linux 8 STIG

v1.0.0 - 11-12-2021

Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

Table of Contents

Terms of Use	1
Overview	28
Intended Audience.....	28
Consensus Guidance.....	28
Typographical Conventions	29
Assessment Status.....	29
Profile Definitions	30
Acknowledgements	32
Recommendations.....	34
1 Initial Setup.....	34
1.1 Filesystem Configuration	35
1.1.1 Disable unused filesystems.....	36
1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated)	37
1.1.1.2 Ensure mounting of vFAT filesystems is limited (Manual).....	39
1.1.1.3 Ensure mounting of squashfs filesystems is disabled (Automated).....	41
1.1.1.4 Ensure mounting of udf filesystems is disabled (Automated).....	43
1.1.2 Ensure /tmp is configured (Automated)	45
1.1.3 Ensure nodev option set on /tmp partition (Automated)	49
1.1.4 Ensure nosuid option set on /tmp partition (Automated)	51
1.1.5 Ensure noexec option set on /tmp partition (Automated)	53
1.1.6 Ensure separate partition exists for /var (Automated)	55
1.1.7 Ensure separate partition exists for /var/tmp (Automated)	57
1.1.8 Ensure nodev option set on /var/tmp partition (Automated)	59
1.1.9 Ensure nosuid option set on /var/tmp partition (Automated)	61
1.1.10 Ensure noexec option set on /var/tmp partition (Automated)	63
1.1.11 Ensure separate partition exists for /var/log (Automated).....	65
1.1.12 Ensure separate partition exists for /var/log/audit (Automated)	67
1.1.13 Ensure separate partition exists for /home (Automated).....	69
1.1.14 Ensure nodev option set on /home partition (Automated).....	71
1.1.15 Ensure nodev option set on /dev/shm partition (Automated).....	73
1.1.16 Ensure nosuid option set on /dev/shm partition (Automated)	75
1.1.17 Ensure noexec option set on /dev/shm partition (Automated)	77
1.1.18 Ensure nodev option set on removable media partitions (Manual)	79
1.1.19 Ensure nosuid option set on removable media partitions (Manual)	81

1.1.20 Ensure noexec option set on removable media partitions (Manual)	83
1.1.21 Ensure sticky bit is set on all world-writable directories (Automated)	85
1.1.22 Disable Automounting (Automated)	87
1.1.23 Disable USB Storage (Automated)	89
1.1.24 Ensure file systems that contain user home directories are mounted with the "nosuid" option (Automated)	91
1.1.25 Ensure the "/boot" directory is mounted with the "nosuid" option (Automated).....	93
1.1.26 Ensure all non-root local partitions are mounted with the "nodev" option (Automated).....	95
1.1.27 Ensure file systems that are being NFS-imported are mounted with the "nodev" option (Automated)	97
1.1.28 Ensure file systems being imported via NFS are mounted with the "noexec" option (Automated)	99
1.1.29 Ensure file systems being imported via NFS are mounted with the "nosuid" option (Automated)	101
1.1.30 Ensure a separate file system/partition has been created for non-privileged local interactive user home directories (Automated)	103
1.1.31 Ensure "/var/log" is mounted with the "nodev" option (Automated)	105
1.1.32 Ensure "/var/log" is mounted with the "nosuid" option (Automated).....	107
1.1.33 Ensure "/var/log" is mounted with the "noexec" option (Automated)	109
1.1.34 Ensure "/var/log/audit" is mounted with the "nodev" option (Automated)	111
1.1.35 Ensure "/var/log/audit" is mounted with the "nosuid" option (Automated)	114
1.1.36 Ensure "/var/log/audit" is mounted with the "noexec" option (Automated)	117
1.1.37 Ensure the "/boot/efi" directory is mounted with the "nosuid" option (Automated).....	120
1.1.38 Ensure file systems that contain user home directories are mounted with the "noexec" option (Automated).....	122
1.2 Configure Software Updates	124
1.2.1 Ensure GPG keys are configured (Manual)	125
1.2.2 Ensure gpgcheck is globally activated (Automated)	126
1.2.3 Ensure package manager repositories are configured (Manual)	128
1.2.4 Ensure DNF is configured to perform a signature check on local packages (Automated).....	129
1.3 Configure sudo	131

1.3.1 Ensure sudo is installed (Automated)	132
1.3.2 Ensure sudo commands use pty (Automated)	134
1.3.3 Ensure sudo log file exists (Automated)	136
1.3.4 Ensure the "/etc/sudoers" file has no occurrences of "NOPASSWD" (Automated).....	138
1.3.5 Ensure the "/etc/sudoers" file has no occurrences of "!authenticate" (Automated).....	140
1.3.6 Ensure the "sudoers" file restricts sudo access to authorized personnel (Automated).....	142
1.3.7 Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation (Automated)	144
1.3.8 Ensure the operating system requires re-authentication when using the "sudo" command to elevate privileges (Automated)	146
1.4 Filesystem Integrity Checking.....	148
1.4.1 Ensure AIDE is installed (Automated)	149
1.4.2 Ensure filesystem integrity is regularly checked (Automated)	151
1.4.3 Ensure Advanced Intrusion Detection Environment (AIDE) is properly configured to use cryptographic mechanisms to protect the integrity of audit tools (Automated).....	154
1.4.4 Ensure the file integrity tool is configured to verify extended attributes (Manual)	157
1.4.5 Ensure the file integrity tool is configured to verify ACLs (Manual)	160
1.5 Secure Boot Settings	162
1.5.1 Ensure permissions on bootloader config are configured (Automated).....	163
1.5.2 Ensure bootloader password is set (Automated).....	166
1.5.3 Ensure authentication required for single user mode (Automated)	169
1.5.4 Ensure the encrypted grub superusers password is set for systems booted with UEFI (Automated)	171
1.5.5 Ensure the encrypted grub superusers password is set for system booted with BIOS (Automated)	173
1.5.6 Ensure the operating system requires authentication for rescue mode (Automated).....	175
1.5.7 Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities (Automated)	177
1.5.8 Ensure GRUB 2 is configured to disable vsyscalls (Automated).....	180
1.5.9 Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities (Automated)	183
1.5.10 Ensure the operating system is configured to boot to the command line (Automated).....	186

1.5.11 Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed (Automated).....	188
1.5.12 Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds (Automated)	190
1.5.13 Ensure a unique name is set as the "superusers" account (UEFI) (Automated).....	192
1.5.14 Ensure a unique name is set as the "superusers" account (BIOS) (Automated).....	194
1.5.15 Ensure the operating system requires authentication upon booting into emergency mode (Automated).....	196
1.6 Additional Process Hardening	198
1.6.1 Ensure core dumps are restricted (Automated).....	198
1.6.2 Ensure address space layout randomization (ASLR) is enabled (Automated)	200
1.6.3 Ensure the operating system disables the storing core dumps (Automated)	202
1.6.4 Ensure the operating system is not configured to acquire, save, or process core dumps (Automated).....	204
1.6.5 Ensure kernel core dumps are disabled unless needed (Automated)	206
1.6.6 Ensure the operating system disables core dumps for all users (Automated)	208
1.6.7 Ensure the operating system disables storing core dumps for all users (Automated).....	210
1.6.8 Ensure the operating system disables core dump backtraces (Automated)	212
1.7 Mandatory Access Control.....	214
1.7.1 Configure SELinux	215
1.7.1.1 Ensure SELinux is installed (Automated)	217
1.7.1.2 Ensure SELinux is not disabled in bootloader configuration (Automated)	218
1.7.1.3 Ensure SELinux policy is configured (Automated)	220
1.7.1.4 Ensure the SELinux state is enforcing (Automated).....	222
1.7.1.5 Ensure no unconfined services exist (Automated)	224
1.7.1.6 Ensure SETroubleshoot is not installed (Automated)	225
1.7.1.7 Ensure the MCS Translation Service (mcstrans) is not installed (Automated).....	226
1.7.1.8 Ensure the operating system has the policycoreutils package installed (Automated).....	227
1.8 Command Line Warning Banners.....	229

1.8.1 Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon (Automated)	230
1.8.2 Ensure message of the day is configured properly (Automated)	235
1.8.3 Ensure local login warning banner is configured properly (Automated)....	237
1.8.4 Ensure remote login warning banner is configured properly (Automated)	239
1.8.5 Ensure permissions on /etc/motd are configured (Automated)	241
1.8.6 Ensure permissions on /etc/issue are configured (Automated)	242
1.8.7 Ensure permissions on /etc/issue.net are configured (Automated).....	243
1.8.8 Ensure the Standard Mandatory DoD Notice and Consent Banner is displayed before granting access to the system via SSH logon (Automated).....	244
1.8.9 Ensure the operating system displays a banner before granting access to the operating system via a graphical user logon (Automated).....	248
1.9 GNOME Display Manager	250
1.9.1 Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon (Automated)	251
1.9.2 Ensure GNOME Display Manager is removed (Manual)	256
1.9.3 Ensure GDM login banner is configured (Automated)	257
1.9.4 Ensure last logged in user display is disabled (Automated)	260
1.9.5 Ensure XDCMP is not enabled (Automated).....	262
1.9.6 Ensure a Standard Mandatory DoD Notice and Consent Banner is displayed via a graphical user logon (Manual)	264
1.9.7 Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface (Automated)	269
1.9.8 Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface (Automated)...	271
1.9.9 Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated (Automated).....	273
1.9.10 Ensure the operating system disables the user logon list for graphical user interfaces (Automated)	275
1.9.11 Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface (Automated)	277
1.9.12 Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface (Automated)	280
1.10 Ensure updates, patches, and additional security software are installed (Manual)	283
1.11 Ensure system-wide crypto policy is not legacy (Automated).....	285

1.12 Ensure system-wide crypto policy is FUTURE or FIPS (Automated)	287
1.13 Ensure the operating system implements DoD-approved encryption (Automated).....	289
1.14 Ensure the operating system prevents unauthorized modification of all information at rest by using disk encryption (Manual).....	292
1.15 Ensure kernel image loading is disabled (Automated)	294
1.16 Ensure the operating system is configured to enable DAC on symlinks (Automated).....	296
1.17 Ensure the operating system is configured to enable DAC on hardlinks (Automated).....	299
1.18 Ensure the operating system is configured to restrict access to the kernel message buffer (Automated).....	302
1.19 Ensure the operating system is configured to prevent kernel profiling by unprivileged users (Automated).....	305
1.20 Ensure the operating system has the packages required for multifactor authentication (Automated)	308
1.21 Ensure the operating system implements certificate status checking for multifactor authentication (Automated)	310
1.22 Ensure the operating system accepts PIV credentials (Automated)	313
1.23 Ensure the NX (no-execution) bit flag is set on the system (Automated)....	315
1.24 Ensure kernel page-table isolation is enabled (Automated)	317
1.25 Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall (Automated)	320
1.26 Ensure the operating system restricts usage of ptrace to descendant processes (Automated).....	322
1.27 Ensure the operating system restricts exposed kernel pointer addresses access (Automated).....	324
1.28 Ensure the operating system disables the ability to load the firewire-core kernel module (Automated)	326
1.29 Ensure the operating system disables the ability to load the USB Storage kernel module (Automated)	328
1.30 Ensure the operating system disables the use of user namespaces (Automated).....	330
1.31 Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service (Automated)	332
1.32 Ensure the "tmux" package installed (Automated)	334
1.33 Ensure the operating system enables hardening for the BPF JIT (Automated)	336

1.34 Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool (Automated)	338
2 Services.....	340
2.1 inetd Services.....	341
2.1.1 Ensure xinetd is not installed (Automated).....	342
2.2 Special Purpose Services.....	343
2.2.1 Time Synchronization.....	344
2.2.1.1 Ensure time synchronization is in use (Manual)	345
2.2.1.2 Ensure chrony is configured (Automated)	347
2.2.1.3 Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server (Automated)	349
2.2.1.4 Ensure the operating system disables the chrony daemon from acting as a server (Automated).....	352
2.2.1.5 Ensure the operating system disables network management of the chrony daemon (Automated)	354
2.2.2 Ensure X Window System is not installed (Automated).....	356
2.2.3 Ensure rsync service is not enabled (Automated)	357
2.2.4 Ensure Avahi Server is not enabled (Automated).....	359
2.2.5 Ensure SNMP Server is not enabled (Automated)	361
2.2.6 Ensure HTTP Proxy Server is not enabled (Automated).....	363
2.2.7 Ensure Samba is not enabled (Automated)	364
2.2.8 Ensure IMAP and POP3 server is not enabled (Automated).....	365
2.2.9 Ensure HTTP server is not enabled (Automated)	367
2.2.10 Ensure FTP Server is not enabled (Automated).....	369
2.2.11 Ensure DNS Server is not enabled (Automated)	371
2.2.12 Ensure NFS is not enabled (Automated)	372
2.2.13 Ensure RPC is not enabled (Automated)	374
2.2.14 Ensure LDAP server is not enabled (Automated).....	376
2.2.15 Ensure DHCP Server is not enabled (Automated)	378
2.2.16 Ensure the telnet-server package is not installed (Automated)	380
2.2.17 Ensure CUPS is not enabled (Automated)	382
2.2.18 Ensure NIS Server is not enabled (Automated)	384
2.2.19 Ensure mail transfer agent is configured for local-only mode (Automated)	386
2.2.20 Ensure the operating system has enabled the hardware random number generator entropy gatherer service (Automated)	388

2.2.21 Ensure automated bug reporting tools are not installed (Automated).....	390
2.2.22 Ensure the sendmail package is not installed (Automated)	392
2.2.23 Ensure the rsh-server package is not installed (Automated)	394
2.2.24 Ensure a camera is not installed (Manual)	396
2.2.25 Ensure the operating system is configured to mask the debug-shell systemd service (Automated)	399
2.2.26 Ensure a TFTP server has not been installed on the system (Automated)	401
2.2.27 Ensure the operating system is configured to prevent unrestricted mail relaying (Automated)	403
2.2.28 Ensure the TFTP daemon is configured to operate in secure mode (Automated).....	405
2.2.29 Ensure an FTP server has not been installed on the system (Automated)	407
2.2.30 Ensure the gssproxy package has not been installed on the system (Automated).....	409
2.2.31 Ensure the iputils package has not been installed on the system (Automated).....	411
2.2.32 Ensure the tuned package has not been installed on the system (Automated).....	413
2.2.33 Ensure the krb5-server package has not been installed on the system (Automated).....	415
2.3 Service Clients	417
2.3.1 Ensure NIS Client is not installed (Automated)	418
2.3.2 Ensure telnet client is not installed (Automated)	420
2.3.3 Ensure LDAP client is not installed (Automated).....	422
3 Network Configuration.....	423
3.1 Network Parameters (Host Only)	424
3.1.1 Ensure IP forwarding is disabled (Automated)	425
3.1.2 Ensure packet redirect sending is disabled (Automated)	427
3.1.3 Ensure the system does not accept router advertisements on IPv6 interfaces, unless the system is a router (Automated).....	429
3.1.4 Ensure the system does not accept router advertisements on IPv6 interfaces by default, unless the system is a router (Automated)	431
3.2 Network Parameters (Host and Router).....	433
3.2.1 Ensure source routed packets are not accepted (Automated).....	434
3.2.2 Ensure ICMP redirects are not accepted (Automated)	437
3.2.3 Ensure secure ICMP redirects are not accepted (Automated)	440

3.2.4 Ensure suspicious packets are logged (Automated)	442
3.2.5 Ensure broadcast ICMP requests are ignored (Automated)	444
3.2.6 Ensure bogus ICMP responses are ignored (Automated)	446
3.2.7 Ensure Reverse Path Filtering is enabled (Automated).....	448
3.2.8 Ensure TCP SYN Cookies is enabled (Automated)	451
3.2.9 Ensure IPv6 router advertisements are not accepted (Automated).....	453
3.2.10 Ensure the operating system does not accept IPv6 ICMP redirect messages (Automated).....	455
3.2.11 Ensure the operating system does not accept IPv6 source-routed packets (Automated).....	457
3.2.12 Ensure the operating system does not accept IPv6 source-routed packets by default (Automated)	459
3.2.13 Ensure the operating system ignores IPv6 ICMP redirect messages (Automated).....	461
3.2.14 Ensure network interfaces are not in promiscuous mode (Automated)...	463
3.2.15 Ensure the operating system does not accept IPv4 ICMP redirect messages (Automated).....	465
3.2.16 Ensure the operating system does not accept IPv4 source-routed packet (Automated).....	467
3.2.17 Ensure the operating system does not accept IPv4 source-routed packets by default (Automated)	469
3.2.18 Ensure the operating system ignores IPv4 ICMP redirect messages (Automated).....	471
3.3 Uncommon Network Protocols	473
3.3.1 Ensure DCCP is disabled (Automated)	474
3.3.2 Ensure SCTP is disabled (Automated)	475
3.3.3 Ensure RDS is disabled (Automated)	477
3.3.4 Ensure TIPC is disabled (Automated)	478
3.3.5 Ensure ATM is disabled (Automated).....	480
3.3.6 Ensure CAN is disabled (Automated).....	482
3.4 Firewall Configuration	484
3.4.1 Ensure Firewall software is installed.....	485
3.4.1.1 Ensure a Firewall package is installed (Automated)	486
3.4.2 Configure firewalld.....	488
3.4.2.1 Ensure firewalld service is enabled and running (Automated)	489
3.4.2.2 Ensure iptables service is not enabled with firewalld (Automated)	491
3.4.2.3 Ensure nftables is not enabled with firewalld (Automated)	493

3.4.2.4 Ensure firewalld default zone is set (Automated)	495
3.4.2.5 Ensure network interfaces are assigned to appropriate zone (Manual) ..	497
3.4.2.6 Ensure firewalld drops unnecessary services and ports (Manual)	499
3.4.2.7 Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems (Manual)	501
3.4.2.8 Ensure "firewalld" is installed (Automated).....	503
3.4.3 Configure nftables	505
3.4.3.1 Ensure iptables are flushed with nftables (Manual).....	509
3.4.3.2 Ensure an nftables table exists (Automated)	511
3.4.3.3 Ensure nftables base chains exist (Automated)	513
3.4.3.4 Ensure nftables loopback traffic is configured (Automated)	515
3.4.3.5 Ensure nftables outbound and established connections are configured (Manual)	517
3.4.3.6 Ensure nftables default deny firewall policy (Automated)	519
3.4.3.7 Ensure nftables service is enabled (Automated)	521
3.4.3.8 Ensure nftables rules are permanent (Automated).....	522
3.4.3.9 Ensure "nftables" is configured to allow rate limits on any connection to the system (Automated).....	525
3.4.4 Configure iptables.....	527
3.4.4.1.1 Ensure iptables loopback traffic is configured (Automated)	530
3.4.4.1.2 Ensure iptables outbound and established connections are configured (Manual)	532
3.4.4.1.3 Ensure iptables firewall rules exist for all open ports (Automated)	534
3.4.4.1.4 Ensure iptables default deny firewall policy (Automated)	536
3.4.4.1.5 Ensure iptables is enabled and active (Automated)	538
3.4.4.2.1 Ensure ip6tables loopback traffic is configured (Automated)	542
3.4.4.2.2 Ensure ip6tables outbound and established connections are configured (Manual)	544
3.4.4.2.3 Ensure ip6tables firewall rules exist for all open ports (Automated)....	546
3.4.4.2.4 Ensure ip6tables default deny firewall policy (Automated)	549
3.4.4.2.5 Ensure ip6tables is enabled and active (Automated)	551
3.4.5 Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services (Manual)	553
3.5 Ensure wireless interfaces are disabled (Automated).....	556
3.6 Disable IPv6 (Manual)	558
3.7 Ensure at least two name servers are configured if using DNS resolution (Automated).....	560

3.8 Ensure Bluetooth is disabled (Automated)	562
4 Logging and Auditing	565
4.1 Configure System Accounting (auditd).....	566
4.1.1 Ensure auditing is enabled.....	567
4.1.1.1 Ensure auditd is installed (Automated).....	568
4.1.1.2 Ensure auditd service is enabled (Automated)	570
4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated).....	572
4.1.1.4 Ensure audit_backlog_limit is sufficient (Automated)	574
4.1.1.5 Ensure the audit service is configured to produce audit records (Automated).....	576
4.1.2 Configure Data Retention	579
4.1.2.1 Ensure audit log storage size is configured (Automated)	580
4.1.2.2 Ensure audit logs are not automatically deleted (Automated)	581
4.1.2.3 Ensure system is disabled when audit logs are full (Automated)	582
4.1.2.4 Ensure the operating system allocates audit record storage capacity (Manual)	583
4.1.2.5 Ensure the operating system has the packages required for offloading audit logs (Automated).....	586
4.1.2.6 Ensure the operating system has the packages required for encrypting offloaded audit logs (Automated).....	588
4.1.2.7 Ensure the audit system off-loads audit records onto a different system or media from the system being audited (Automated)	590
4.1.2.8 Ensure the audit system is configured to take an appropriate action when the internal event queue is full (Automated).....	592
4.1.2.9 Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited (Automated)	594
4.1.2.10 Ensure the the operating system authenticates the remote logging server for off-loading audit logs (Automated).....	597
4.1.2.11 Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity (Automated).....	599
4.1.3 Ensure changes to system administration scope (sudoers) is collected (Automated).....	601
4.1.4 Ensure the SA and ISSO are notified in the event of an audit processing failure (Automated)	603
4.1.5 Ensure the SA and ISSO are notified when the audit storage volume is full (Automated).....	605

4.1.6 Ensure an audit event is generated for any successful/unsuccessful use of the "chage" command (Automated)	607
4.1.7 Ensure the operating system is configured to audit the execution of the "fremovexattr" system call (Automated).....	609
4.1.8 Ensure the operating system is configured to audit the execution of the "fsetxattr" system call (Automated)	611
4.1.9 Ensure the operating system is configured to audit the execution of the "lsetxattr" system call (Automated)	613
4.1.10 Ensure the operating system is configured to audit the execution of the "removexattr" system call (Automated)	615
4.1.11 Ensure the operating system is configured to audit the execution of the "lremovexattr" system call (Automated).....	617
4.1.12 Ensure the operating system generates audit records when successful/unsuccessful attempts to use the "su" command by performing the following command to check the file system rules in "/etc/audit/audit.rules" (Automated).....	619
4.1.13 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/" (Automated)	621
4.1.14 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers" (Automated)	623
4.1.15 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow" (Automated)	625
4.1.16 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd" (Automated).....	627
4.1.17 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow" (Automated)	629
4.1.18 Ensure the audit system prevents unauthorized changes to logon UIDs (Automated).....	631
4.1.19 Ensure the audit system prevents unauthorized changes (Automated) ...	633
4.1.20 Ensure the operating system takes the appropriate action when the audit storage volume is full (Automated)	635
4.1.21 Ensure the operating system takes the appropriate action when the audit storage volume is full (Automated)	637
4.1.22 Ensure login and logout events are collected (Automated)	639
4.1.23 Ensure the operating system takes the appropriate action when an audit processing failure occurs (Automated)	641

4.1.24 Ensure session initiation information is collected (Automated)	643
4.1.25 Ensure events that modify date and time information are collected (Automated).....	645
4.1.26 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	647
4.1.27 Ensure events that modify the system's network environment are collected (Automated).....	649
4.1.28 Ensure discretionary access control permission modification events are collected (Automated)	652
4.1.29 Ensure unsuccessful unauthorized file access attempts are collected (Automated).....	656
4.1.30 Ensure events that modify user/group information are collected (Automated).....	659
4.1.31 Ensure successful file system mounts are collected (Automated).....	661
4.1.32 Ensure use of privileged commands is collected (Automated)	664
4.1.33 Ensure file deletion events by users are collected (Automated)	667
4.1.34 Ensure kernel module loading and unloading is collected (Automated) ..	670
4.1.35 Ensure system administrator actions (sudolog) are collected (Automated)	673
4.1.36 Ensure the audit configuration is immutable (Automated).....	675
4.1.37 Ensure the operating system audits the execution of privileged functions (Automated).....	677
4.1.38 Ensure the operating system's audit daemon is configured to include local events (Automated)	679
4.1.39 Ensure the operating system's audit daemon is configured to label all off-loaded audit logs (Automated)	681
4.1.40 Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk (Automated)	683
4.1.41 Ensure the operating system's audit logs have a mode of "0600" or less permissive (Automated)	685
4.1.42 Ensure the operating system's audit logs are owned by "root" (Automated)	687
4.1.43 Ensure the audit logs are group-owned by "root" (Automated).....	689
4.1.44 Ensure the audit log directory is owned by "root" to prevent unauthorized read access (Automated)	691
4.1.45 Ensure the audit log directory is group-owned by "root" to prevent unauthorized read access (Automated).....	693
4.1.46 Ensure the audit log directories have a mode of "0700" or less permissive by first determining where the audit logs are stored (Automated).....	695

4.1.47 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chcon" command (Automated).....	697
4.1.48 Ensure the operating system is configured to audit the execution of the "setxattr" system call (Automated).....	699
4.1.49 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd" (Automated).....	701
4.1.50 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group" (Automated)	703
4.1.51 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-agent" (Automated)	705
4.1.52 Ensure an audit event is generated for any successful/unsuccessful use of the "passwd" command (Automated).....	707
4.1.53 Ensure an audit event is generated for any successful/unsuccessful use of the "mount" command (Automated).....	709
4.1.54 Ensure an audit event is generated for any successful/unsuccessful use of the "umount" command (Automated)	711
4.1.55 Ensure an audit event is generated for any successful/unsuccessful use of the "mount" syscall (Automated)	713
4.1.56 Ensure an audit event is generated for any successful/unsuccessful use of the "unix_update" (Automated)	715
4.1.57 Ensure an audit event is generated for any successful/unsuccessful use of "postdrop" (Automated)	717
4.1.58 Ensure an audit event is generated for any successful/unsuccessful use of "postqueue" (Automated).....	719
4.1.59 Ensure an audit event is generated for any successful/unsuccessful use of "semanage" (Automated).....	721
4.1.60 Ensure an audit event is generated for any successful/unsuccessful use of "setfiles" (Automated)	723
4.1.61 Ensure an audit event is generated for any successful/unsuccessful use of "userhelper" (Automated).....	725
4.1.62 Ensure an audit event is generated for any successful/unsuccessful use of "setsebool" (Automated).....	727
4.1.63 Ensure an audit event is generated for any successful/unsuccessful use of "unix_chkpwd" (Automated)	729
4.1.64 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-keysign" (Automated)	731
4.1.65 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "setfacl" command (Automated)...	733

4.1.66 Ensure an audit event is generated for any successful/unsuccessful use of the "pam_timestamp_check" command (Automated)	735
4.1.67 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "newgrp" command (Automated)	737
4.1.68 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "init_module" command (Automated)	739
4.1.69 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rename" command (Automated)	741
4.1.70 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "renameat" command (Automated)	743
4.1.71 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rmdir" command (Automated)....	745
4.1.72 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlink" command (Automated)...	747
4.1.73 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlinkat" command (Automated)	749
4.1.74 Ensure an audit event is generated for any successful/unsuccessful use of the "gpasswd" command (Automated)	751
4.1.75 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "finit_module" command (Automated).....	753
4.1.76 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "delete_module" command (Automated).....	755
4.1.77 Ensure an audit event is generated for any successful/unsuccessful use of the "crontab" command (Automated)	757
4.1.78 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chsh" command (Automated)	759
4.1.79 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "truncate" command (Automated)	761
4.1.80 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "openat" command (Automated)..	764
4.1.81 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open" system call (Automated) ...	767
4.1.82 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open_by_handle_at" system call (Automated).....	770

4.1.83 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ftruncate" command (Automated)	773
4.1.84 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "creat" system call (Automated) ...	776
4.1.85 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chown" command (Automated)..	779
4.1.86 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chmod" command (Automated)..	781
4.1.87 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "lchown" system call (Automated)	783
4.1.88 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchownat" system call (Automated)	785
4.1.89 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchown" system call (Automated)	787
4.1.90 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmod" system call (Automated)	789
4.1.91 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmodat" system call (Automated)	791
4.1.92 Ensure an audit event is generated for any successful/unsuccessful use of the "sudo" command (Automated)	793
4.1.93 Ensure an audit event is generated for any successful/unsuccessful use of the "usermod" command (Automated)	795
4.1.94 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chacl" command (Automated)	797
4.1.95 Ensure the operating system is configured to audit the execution of the module management program "kmod" (Automated).....	799
4.1.96 Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "faillock" file occur (Automated).801	
4.1.97 Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "lastlog" file (Automated)	804
4.1.98 Ensure the operating system enables auditing of processes that start prior to the audit daemon (Automated).....	806
4.1.99 Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon (Automated)	809

4.1.100 Ensure the operating system enables Linux audit logging of the USBGuard daemon (Automated)	812
4.1.101 Ensure the files in directory "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive (Automated).....	814
4.1.102 Ensure the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode (Automated).....	816
4.1.103 Ensure the audit tools are owned by "root" to prevent any unauthorized access, deletion, or modification (Automated).....	818
4.1.104 Ensure the audit tools are group-owned by "root" to prevent any unauthorized access, deletion, or modification (Automated)	820
4.1.105 Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent (Automated)	822
4.2 Configure Logging.....	824
4.2.1 Configure rsyslog	825
4.2.1.1 Ensure rsyslog is installed (Automated)	826
4.2.1.2 Ensure the rsyslog service is enabled and active (Automated)	827
4.2.1.3 Ensure the operating system monitors all remote access methods (Automated).....	829
4.2.1.4 Ensure rsyslog Service is enabled (Automated).....	831
4.2.1.5 Ensure rsyslog default file permissions configured (Automated)	832
4.2.1.6 Ensure logging is configured (Manual)	833
4.2.1.7 Ensure rsyslog is configured to send logs to a remote log host (Automated)	835
4.2.1.8 Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)	837
4.2.1.9 Ensure "rsyslog" is configured to log cron events (Automated)	839
4.2.2 Configure journald.....	841
4.2.2.1 Ensure journald is configured to send logs to rsyslog (Automated)	842
4.2.2.2 Ensure journald is configured to compress large log files (Automated) ..	844
4.2.2.3 Ensure journald is configured to write logfiles to persistent disk (Automated).....	846
4.2.3 Ensure permissions on all logfiles are configured (Automated)	848
4.3 Ensure logrotate is configured (Manual)	849
4.4 Ensure administrators are notified if an audit processing failure occurs by modifying "/etc/aliases" (Automated)	850
5 Access, Authentication and Authorization.....	852
5.1 Configure cron	853

5.1.1 Ensure cron daemon is enabled (Automated)	854
5.1.2 Ensure permissions on /etc/crontab are configured (Automated)	855
5.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)	856
5.1.4 Ensure permissions on /etc/cron.daily are configured (Automated).....	858
5.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated).....	859
5.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated) ...	861
5.1.7 Ensure permissions on /etc/cron.d are configured (Automated)	863
5.1.8 Ensure at/cron is restricted to authorized users (Automated)	865
5.2 SSH Server Configuration.....	868
5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	
.....	869
5.2.2 Ensure SSH private key files have a passcode (Manual).....	870
5.2.3 Ensure SSH access is limited (Automated)	872
5.2.4 Ensure permissions on SSH private host key files are configured (Automated).....	875
5.2.5 Ensure permissions on SSH public host key files are configured (Automated)	
.....	878
5.2.6 Ensure SSH LogLevel is appropriate (Automated)	881
5.2.7 Ensure SSH X11 forwarding is disabled (Automated).....	883
5.2.8 Ensure SSH MaxAuthTries is set to 4 or less (Automated)	885
5.2.9 Ensure SSH IgnoreRhosts is enabled (Automated)	887
5.2.10 Ensure SSH HostbasedAuthentication is disabled (Automated)	889
5.2.11 Ensure SSH root login is disabled (Automated)	891
5.2.12 Ensure SSH PermitEmptyPasswords is disabled (Automated).....	893
5.2.13 Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity (Automated).....	895
5.2.14 Ensure SSH PermitUserEnvironment is disabled (Automated)	898
5.2.15 Ensure SSH Idle Timeout Interval is configured (Automated)	900
5.2.16 Ensure SSH LoginGraceTime is set to one minute or less (Automated)	903
5.2.17 Ensure SSH warning banner is configured (Automated).....	905
5.2.18 Ensure SSH PAM is enabled (Automated)	906
5.2.19 Ensure SSH AllowTcpForwarding is disabled (Automated).....	908
5.2.20 Ensure SSH MaxStartups is configured (Automated)	910
5.2.21 Ensure SSH MaxSessions is set to 4 or less (Automated)	912

5.2.22 Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms (Automated)	914
5.2.23 Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms (Automated)	917
5.2.24 Ensure the SSH server uses strong entropy (Automated)	919
5.2.25 Ensure system-wide crypto policy is not over-ridden (Automated)	921
5.2.26 Ensure the SSH daemon performs strict mode checking of home directory configuration files (Automated)	922
5.2.27 Ensure the SSH daemon performs compression after a user successfully authenticates (Automated)	924
5.2.28 Ensure the SSH daemon does not allow authentication using known host's authentication (Automated)	926
5.2.29 Ensure the SSH daemon does not allow Kerberos authentication (Automated)	928
5.2.30 Ensure null passwords cannot be used (Automated)	930
5.2.31 Ensure SSH provides users with feedback on when account accesses last occurred (Automated)	932
5.2.32 Ensure SSH is loaded and active (Automated)	934
5.2.33 Ensure the SSH server is configured to force frequent session key renegotiation (Automated)	936
5.2.34 Ensure the SSH daemon prevents remote hosts from connecting to the proxy display (Automated)	938
5.2.35 Ensure system-wide crypto policies are in effect (Automated)	940
5.2.36 Ensure the SSH daemon does not allow GSSAPI authentication (Automated)	942
5.2.37 Ensure SSH is installed (Automated)	944
5.2.38 Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity (Automated)	946
5.3 Configure authselect	949
5.3.1 Create custom authselect profile (Automated)	950
5.3.2 Select authselect profile (Automated)	951
5.3.3 Ensure authselect includes with-faillock (Automated)	953
5.4 Configure PAM.....	955
5.4.1 Ensure password creation requirements are configured (Automated)	956
5.4.2 Ensure the system locks an account after three unsuccessful logon attempts (Automated)	959
5.4.3 Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts within 15 minutes (Automated)	962

5.4.4 Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes (Automated).....	964
5.4.5 Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts (Automated)	967
5.4.6 Ensure lockout for failed password attempts is configured (Automated) ..	969
5.4.7 Ensure password reuse is limited (Automated)	971
5.4.8 Ensure password hashing algorithm is SHA-512 (Automated).....	973
5.4.9 Ensure a minimum number of hash rounds is configured (Automated)	975
5.4.10 Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes until released by an administrator (Automated).....	977
5.4.11 Ensure the "/etc/security/faillock.conf" file is configured to lock an account until released by an administrator after three unsuccessful logon attempts (Automated)	980
5.4.12 Ensure the faillock directory contents persist after a reboot (Automated)	982
5.4.13 Ensure the "/etc/security/faillock.conf" file is configured to use a non-default faillock directory to ensure contents persist after reboot (Automated) .	985
5.4.14 Ensure the system prevents informative messages to the user about logon information (Automated)	987
5.4.15 Ensure the "/etc/security/faillock.conf" file is configured to prevent informative messages about logon attempts (Automated)	990
5.4.16 Ensure the system logs user name information when unsuccessful logon attempts occur (Automated)	992
5.4.17 Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur (Automated)	995
5.4.18 Ensure the system includes the root account when locking an account after three unsuccessful logon attempts within a period of 15 minutes (Automated)	997
5.4.19 Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur (Automated)	1000
5.4.20 Ensure the operating system prohibits password reuse for a minimum of five generations (Automated)	1002
5.4.21 Ensure the operating system uses multifactor authentication for local access to accounts (Automated)	1004
5.4.22 Ensure the date and time of the last successful account logon upon logon is displayed (Automated)	1007
5.4.23 Ensure the "pam_unix.so" module is configured to use sha512 (Automated)	1009
5.4.24 Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/system-auth" file (Automated)	1011

5.4.25 Ensure blank or null passwords in the "system-auth" file cannot be used (Automated).....	1013
5.4.26 Ensure blank or null passwords in the "password-auth" file cannot be used (Automated).....	1015
5.4.27 Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/password-auth" file (Automated)	1017
5.5 User Accounts and Environment	1019
5.5.1 Set Shadow Password Suite Parameters	1020
5.5.1.1 Ensure password expiration is 365 days or less (Automated).....	1021
5.5.1.2 Ensure the shadow password suite configuration is set to encrypt password with a FIPS 140-2 approved cryptographic hashing algorithm. (Automated).....	1023
5.5.1.3 Ensure the value of the "maxrepeat" option in "/etc/security/pwquality.conf" is "3" (Automated)	1025
5.5.1.4 Ensure the value of the "difok" option in "/etc/security/pwquality.conf" is "8" (Automated)	1027
5.5.1.5 Ensure the value of the "minclass" option in "/etc/security/pwquality.conf" is "4" (Automated)	1029
5.5.1.6 Ensure the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" is "4" (Automated)	1031
5.5.1.7 Ensure the value for "dcredit" in "/etc/security/pwquality.conf" is "-1" (Automated).....	1033
5.5.1.8 Ensure the value for "lcredit" in "/etc/security/pwquality.conf" is "-1" (Automated).....	1035
5.5.1.9 Ensure the value for "ucredit" in "/etc/security/pwquality.conf" is "-1" (Automated).....	1037
5.5.1.10 Ensure the operating system uses "pwquality" to enforce the password complexity rules (Automated).....	1039
5.5.1.11 Ensure minimum days between password changes is 7 or more (Automated).....	1041
5.5.1.12 Ensure password expiration warning days is 7 or more (Automated)	1043
5.5.1.13 Ensure inactive password lock is 30 days or less (Automated)	1045
5.5.1.14 Ensure all users last password change date is in the past (Automated)	1047
5.5.1.15 Ensure the minimum time period between password changes for each user account is one day or greater (Automated).....	1048
5.5.1.16 Ensure the operating system enforces 24 hours/1 day as the minimum password lifetime for new user accounts (Automated)	1050
5.5.1.17 Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts (Automated)	1052

5.5.1.18 Ensure the maximum time period for existing passwords is restricted to 60 days (Automated)	1054
5.5.1.19 Ensure the operating system enforces a minimum 15-character password length (Automated)	1056
5.5.1.20 Ensure the operating system enforces a minimum 15-character password length for new user accounts (Automated)	1058
5.5.1.21 Ensure the value for "ocredit" in "/etc/security/pwquality.conf" is "-1" (Automated)	1060
5.5.1.22 Ensure the operating system prevents the use of dictionary words for passwords (Automated)	1062
5.5.1.23 Ensure the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt (Automated)	1064
5.5.2 Ensure system accounts are secured (Automated)	1066
5.5.3 Ensure default user shell timeout is 900 seconds or less (Automated)	1068
5.5.4 Ensure the interactive user account passwords are using a strong password hash (Automated)	1071
5.5.5 Ensure default group for the root account is GID 0 (Automated)	1073
5.5.6 Ensure default user umask is 027 or more restrictive (Automated)	1074
5.5.7 Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity (Automated)	1079
5.5.8 Ensure emergency accounts have been provisioned with an expiration date of 72 hours (Manual)	1081
5.5.9 Ensure the default umask for all local interactive users is "077" (Manual)	1083
5.5.10 Ensure the umask default for installed shells is "077" (Automated)	1085
5.5.11 Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files (Automated)	1087
5.6 Ensure root login is restricted to system console (Manual)	1089
5.7 Ensure PKI-based authentication has valid certificates (Manual)	1090
5.8 Ensure access to the su command is restricted (Automated)	1093
5.9 Ensure the operating system prevents system daemons from using Kerberos for authentication (Automated)	1095
5.10 Ensure the krb5-workstation package has not been installed on the system (Automated)	1097
5.11 Ensure SSSD prohibits the use of cached authentications after one day (Automated)	1099
5.12 Ensure "fapolicyd" is installed (Automated)	1101

5.13 Ensure USBGuard has a policy configured (Manual)	1103
5.14 Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms (Automated)	1105
5.15 Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption (Automated)	1108
5.16 Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions (Automated)	1110
5.17 Ensure "fapolicyd" is enabled and running (Automated)	1112
5.18 Ensure "fapolicyd" employs a deny-all, permit-by-exception policy (Automated).....	1114
5.19 Ensure USBGuard is installed on the operating system (Automated)	1117
5.20 Ensure the operating system has enabled the use of the USBGuard (Automated).....	1119
6 System Maintenance.....	1121
6.1 System File Permissions.....	1122
6.1.1 Audit system file permissions (Manual)	1123
6.1.2 Ensure permissions on /etc/passwd are configured (Automated)	1126
6.1.3 Ensure permissions on /etc/passwd- are configured (Automated).....	1127
6.1.4 Ensure permissions on /etc/shadow are configured (Automated).....	1128
6.1.5 Ensure permissions on /etc/shadow- are configured (Automated)	1129
6.1.6 Ensure permissions on /etc/gshadow are configured (Automated).....	1130
6.1.7 Ensure permissions on /etc/gshadow- are configured (Automated)	1131
6.1.8 Ensure permissions on /etc/group are configured (Automated).....	1132
6.1.9 Ensure permissions on /etc/group- are configured (Automated)	1133
6.1.10 Ensure the root account is the only account that has unrestricted access to the operating system (Automated).....	1134
6.1.11 Ensure no world writable files exist (Automated)	1136
6.1.12 Ensure no unowned files or directories exist (Automated)	1138
6.1.13 Ensure no ungrouped files or directories exist (Automated)	1139
6.1.14 Ensure all public directories are owned by root or a system account (Manual)	1140
6.1.15 Audit SUID executables (Manual)	1142
6.1.16 Audit SGID executables (Manual)	1143
6.1.17 Ensure the "/var/log/messages" file has mode "0640" or less permissive (Automated).....	1145
6.1.18 Ensure the "/var/log/messages" file is owned by root (Automated).....	1147

6.1.19 Ensure the "/var/log/messages" file is group-owned by root (Automated)	1149
6.1.20 Ensure the "/var/log" directory has a mode of "0755" or less (Automated)	1151
6.1.21 Ensure the "/var/log" directory is owned by root (Automated)	1153
6.1.22 Ensure the "/var/log" directory is group-owned by root (Automated)	1155
6.1.23 Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories have mode "0755" or less permissive (Automated)	1157
6.1.24 Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are owned by "root" (Automated)	1159
6.1.25 Ensure the system commands contained in "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are group-owned by "root" (Manual)	1161
6.1.26 Ensure the system-wide shared library files contained in the "/lib, /lib64, /usr/lib, /usr/lib64" directories have mode "0755" or less permissive (Automated)	1163
6.1.27 Ensure the system-wide shared library files are owned by "root" (Automated)	1165
6.1.28 Ensure the system-wide shared library files are group-owned by "root" (Manual)	1167
6.1.29 Ensure world-writable directories are owned by root, sys, bin, or an application user (Manual)	1169
6.1.30 Ensure world-writable directories are group-owned by root, sys, bin, or an application group (Manual)	1171
6.1.31 Ensure local initialization files do not execute world-writable programs (Manual)	1173
6.1.32 Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer (Automated)	1175
6.1.33 Ensure the operating system prevents users from disabling the tmux terminal multiplexer (Automated)	1177
6.1.34 Ensure the operating system enables a user's session lock until that user re-establishes access (Automated)	1179
6.1.35 Ensure the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces (Automated)	1181
6.1.36 Ensure the operating system initiates a session lock after 15 minutes of inactivity (Automated)	1183
6.1.37 Ensure all accounts on the system are assigned to an active system, application, or user account (Manual)	1185

6.2 User and Group Settings	1187
6.2.1 Ensure password fields are not empty (Automated).....	1188
6.2.2 Ensure no legacy "+" entries exist in /etc/passwd (Automated).....	1189
6.2.3 Ensure root PATH Integrity (Automated)	1190
6.2.4 Ensure no legacy "+" entries exist in /etc/shadow (Automated)	1192
6.2.5 Ensure no legacy "+" entries exist in /etc/group (Automated)	1193
6.2.6 Ensure root is the only UID 0 account (Automated)	1194
6.2.7 Ensure users' home directories permissions are 750 or more restrictive (Automated).....	1195
6.2.8 Ensure emergency accounts have been provisioned with an expiration date of 72 hours (Manual).....	1197
6.2.9 Ensure users own their home directories (Automated).....	1199
6.2.10 Ensure users' dot files are not group or world writable (Automated)....	1201
6.2.11 Ensure no users have .forward files (Automated).....	1203
6.2.12 Ensure no users have .netrc files (Automated).....	1205
6.2.13 Ensure users' .netrc Files are not group or world accessible (Automated)	1207
6.2.14 Ensure no users have .rhosts files (Automated)	1210
6.2.15 Ensure all groups in /etc/passwd exist in /etc/group (Automated).....	1212
6.2.16 Ensure no duplicate UIDs exist (Automated)	1213
6.2.17 Ensure no duplicate GIDs exist (Automated)	1215
6.2.18 Ensure no duplicate user names exist (Automated)	1216
6.2.19 Ensure no duplicate group names exist (Automated)	1217
6.2.20 Ensure shadow group is empty (Automated)	1218
6.2.21 Ensure all users' home directories exist (Automated)	1219
6.2.22 Ensure the assigned home directory of all local interactive users is group-owned by that user's primary GID (Automated)	1221
6.2.23 Ensure the assigned home directory of all local interactive users exists (Automated).....	1223
6.2.24 Ensure all local interactive users are assigned a home directory upon creation (Automated).....	1225
6.2.25 Ensure all local initialization files have a mode of "0740" or less permissive (Automated).....	1227
6.2.26 Ensure all local files and directories have a valid owner (Automated) ..	1229
6.2.27 Ensure all local files and directories have a valid group (Automated) ...	1231
6.2.28 Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file (Manual)	1233

6.2.29 Ensure file executable search path statements do not share sensitive home directory information (Manual)	1235
6.2.30 Ensure local interactive users have a home directory assigned (Automated)	1237
6.2.31 Ensure the operating system limits the number of concurrent sessions to "10" for all accounts and/or account types (Automated)	1239
6.2.32 Ensure the operating system enables a user's session lock until that user re-establishes access (Automated)	1241
6.2.33 Ensure the operating system enables the user to initiate a session lock (Automated)	1243
6.2.34 Ensure the operating system prevents a user from overriding settings for graphical user interfaces (Automated)	1245
6.2.35 Ensure all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750" (Automated)	1248
6.2.36 Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of (Automated)	1250
6.2.37 Ensure temporary accounts have been provisioned with an expiration date of 72 hours (Manual)	1252
6.3 Ensure the operating system removes all software components after updated versions have been installed (Automated)	1254
6.4 Ensure there are no ".shosts" files on the operating system (Automated) ..	1256
6.5 Ensure there are no "shosts.equiv" files on the operating system (Automated)	1258
Appendix: Recommendation Summary Table	1260
Appendix: CIS Controls v7 IG 1 Mapped Recommendations	1286
Appendix: CIS Controls v7 IG 2 Mapped Recommendations	1301
Appendix: CIS Controls v7 IG 3 Mapped Recommendations	1322
Appendix: CIS Controls v8 IG 1 Mapped Recommendations	1344
Appendix: CIS Controls v8 IG 2 Mapped Recommendations	1358
Appendix: CIS Controls v8 IG 3 Mapped Recommendations	1380
Appendix: Change History	1402

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Red Hat Enterprise Linux 8 systems running on x86_64 platforms. This Benchmark was tested against Red Hat Enterprise Linux 8.4

The guidance within broadly assumes that operations are being performed as the root user. Operations performed using sudo instead of the root user may produce unexpected results, or fail to make the intended changes to the system. Non-root users may not be able to access certain areas of the system, especially after remediation has been performed. It is advisable to verify root users path integrity and the integrity of any programs being run prior to execution of commands and scripts included in this benchmark.

To obtain the latest version of this guide, please visit <http://workbench.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Red Hat Enterprise Linux 8 on x86_64 platforms.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
Stylized Monospace font	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<i><italic font in brackets></i>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Server**

Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

This profile is intended for servers.

- **Level 2 - Server**

This profile extends the "Level 1 - Server" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for servers.

- **Level 1 - Workstation**

Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

This profile is intended for workstations.

- **Level 2 - Workstation**

This profile extends the "Level 1 - Workstation" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for workstations.

- **STIG**

Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where following STIG security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for servers and workstations.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

This benchmark is based upon previous Linux benchmarks published and would not be possible without the contributions provided over the history of all of these benchmarks. The CIS community thanks everyone who has contributed to the Linux benchmarks.

Contributor

Andrew Dannenberger

Anurag Pal

Bill Erickson

Bradley Hieber

Dave Billing

Dominic Pace

Elliot Anderson

Ely Pinto

Fredrik Silverskär

James Trigg

Joy Latten

Kenneth Karlsson

Kirill Antonenko

Koen Laevens

Marcelo Cerri

Mark Birch

Mark Hesse

Martinus Nel

Martynas Brijunas

Michel Verbraak

Mike Saubier

Mike Thompson

Pradeep R B

Rael Daruszka

Rakesh Jain

Robert Thomas

Ron Colvin

Thomas Sjögren

Tom Pietschmann

Vineetha Hari Pai

William E. Triest III

Editor

Jonathan Lewis Christopherson
Eric Pinnell
Justin Brown

Recommendations

1 Initial Setup

Items in this section are advised for all systems, but may be difficult or require extensive preparation after the initial setup of the system.

1.1 Filesystem Configuration

Directories that are used for system-wide functions can be further protected by placing them on separate partitions. This provides protection for resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use. Users' data can be stored on separate partitions and have stricter mount options. A user partition is a filesystem that has been established for use by the users and does not contain software for system operations.

The recommendations in this section are easier to perform during initial system installation. If the system is already installed, it is recommended that a full backup be performed before repartitioning the system.

Note: If you are repartitioning a system that has already been installed, make sure the data has been copied over to the new partition, unmount it and then remove the data from the directory that was in the old partition. Otherwise it will still consume space in the old partition that will be masked when the new filesystem is mounted. For example, if a system is in single-user mode with no filesystems mounted and the administrator adds a lot of data to the `/tmp` directory, this data will still consume space in `/` once the `/tmp` filesystem is mounted unless it is removed first.

1.1.1 Disable unused filesystems

A number of uncommon filesystem types are supported under Linux. Removing support for unneeded filesystem types reduces the local attack surface of the system. If a filesystem type is not needed it should be disabled. Native Linux file systems are designed to ensure that built-in security controls function as expected. Non-native filesystems can lead to unexpected consequences to both the security and functionality of the system and should be used with caution. Many filesystems are created for niche use cases and are not maintained and supported as the operating systems are updated and patched. Users of non-native filesystems should ensure that there is attention and ongoing support for them, especially in light of frequent operating system changes.

Standard network connectivity and Internet access to cloud storage may make the use of non-standard filesystem formats to directly attach heterogeneous devices much less attractive.

Note: This should not be considered a comprehensive list of filesystems. You may wish to consider additions to those listed here for your environment.

1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `cramfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A `cramfs` image can be used without having to first decompress the image.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v cramfs  
install /bin/true  
  
# lsmod | grep cramfs  
  
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vim /etc/modprobe.d/cramfs.conf`
and add the following line:

```
install cramfs /bin/true
```

Run the following command to unload the `cramfs` module:

```
# rmmod cramfs
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230498

Rule ID: SV-230498r627750_rule

STIG ID: RHEL-08-040025

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.1.2 Ensure mounting of vFAT filesystems is limited (Manual)

Profile Applicability:

- Level 2 - Workstation
- Level 2 - Server

Description:

The `vFAT` filesystem format is primarily used on older windows systems and portable USB drives or flash modules. It comes in three types `FAT12`, `FAT16`, and `FAT32` all of which are supported by the `vfat` kernel module.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Impact:

The `FAT` filesystem format is used by UEFI systems for the EFI boot partition. Disabling the `vfat` module can prevent boot on UEFI systems.

`FAT` filesystems are often used on portable USB sticks and other flash media which are commonly used to transfer files between workstations, removing VFAT support may prevent the ability to transfer files in this way.

Audit:

If utilizing UEFI the `vFAT` filesystem format is required. If this case, ensure that the `vFAT` filesystem is only used where appropriate

Run the following command

```
grep -E -i '\$vfat\s' /etc/fstab
```

And review that any output is appropriate for your environment

If not utilizing UEFI

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v vfat  
install /bin/true  
  
# lsmod | grep vfat  
<No output>
```

Remediation:

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf
Example: vim /etc/modprobe.d/vfat.conf

```
install vfat /bin/true
```

Run the following command to unload the vfat module:

```
# rmmod vfat
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.1.3 Ensure mounting of squashfs filesystems is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `squashfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems (similar to `cramfs`). A `squashfs` image can be used without having to first decompress the image.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v squashfs  
install /bin/true  
  
# lsmod | grep squashfs  
  
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vim /etc/modprobe.d/squashfs.conf`
and add the following line:

```
install squashfs /bin/true
```

Run the following command to unload the `squashfs` module:

```
# rmmod squashfs
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.1.4 Ensure mounting of udf filesystems is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `udf` filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v udf
install /bin/true
# lsmod | grep udf
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vim /etc/modprobe.d/udf.conf`
and add the following line:

```
install udf /bin/true
```

Run the following command to unload the `udf` module:

```
# rmmod udf
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.2 Ensure /tmp is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `/tmp` directory is a world-writable directory used for temporary storage by all users and some applications.

Rationale:

Making `/tmp` its own file system allows an administrator to set the `noexec` option on the mount, making `/tmp` useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system setuid program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

This can be accomplished by either mounting `tmpfs` to `/tmp`, or creating a separate partition for `/tmp`.

Impact:

Since the `/tmp` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition.

Running out of `/tmp` space is a problem regardless of what kind of filesystem lies under it, but in a default installation a disk-based `/tmp` will essentially have the whole disk available, as it only creates a single `/` partition. On the other hand, a RAM-based `/tmp` as with `tmpfs` will almost certainly be much smaller, which can lead to applications filling up the filesystem much more easily.

`/tmp` utilizing `tmpfs` can be resized using the `size={size}` parameter on the Options line on the `tmp.mount` file

Audit:

Run the following command and verify output shows /tmp is mounted:

```
# mount | grep -E '\s/tmp\s'  
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

If /etc/fstab is used: run the following command and verify that tmpfs has been mounted to tmpfs, or a system partition has been created for /tmp

```
# grep -E '\s/tmp\s' /etc/fstab | grep -E -v '^#\s*#'  
tmpfs    /tmp      tmpfs    defaults,noexec,nosuid,nodev 0      0
```

Or

If systemd tmp.mount file is used: run the following command and verify that tmp.mount is enabled:

```
# systemctl is-enabled tmp.mount  
enabled
```

Remediation:

Create or update an entry for `/tmp` in either `/etc/fstab` **OR** in a `systemd tmp.mount` file:

If `/etc/fstab` is used: configure `/etc/fstab` as appropriate.

Example:

```
tmpfs    /tmp     tmpfs      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/tmp`

```
# mount -o remount,noexec,nodev,nosuid /tmp
```

Or

If `systemd tmp.mount` file is used:

Run the following command to create the file `/etc/systemd/system/tmp.mount` if it doesn't exist:

```
# [ ! -f /etc/systemd/system/tmp.mount ] && cp -v  
/usr/lib/systemd/system/tmp.mount /etc/systemd/system/
```

Edit the file `/etc/systemd/system/tmp.mount`:

```
[Mount]  
What=tmpfs  
Where=/tmp  
Type=tmpfs  
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to reload the `systemd` daemon:

```
# systemctl daemon-reload
```

Run the following command to unmask and start `tmp.mount`:

```
# systemctl unmask tmp.mount  
# systemctl --now enable tmp.mount
```

References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>
2. <https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/>

Additional Information:

If an entry for /tmp exists in /etc/fstab it will take precedence over entries in the tmp.mount file

BUG 1667065* There is currently a bug in RHEL 8 when attempting to use systemd tmp.mount please reference link below

https://bugzilla.redhat.com/show_bug.cgi?id=1667065

Red Hat Enterprise Linux 8 Security Technical Implementation Guide
Version 1, Release: 3 Benchmark Date: 23 Jul 2021
Vul ID: V-230295
Rule ID: SV-230295r627750_rule
STIG ID: RHEL-08-010543
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	9.1 Associate Active Ports, Services and Protocols to Asset Inventory Associate active ports, services and protocols to the hardware assets in the asset inventory.		●	●

1.1.3 Ensure nodev option set on /tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/tmp` filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices in `/tmp`.

Audit:

Verify that the `nodev` option is set if a `/tmp` partition exists

Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/tmp\s' | grep -v nodev
```

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/tmp` partition. See the `fstab(5)` manual page for more information.

Run the following command to remount `/tmp`:

```
# mount -o remount,nodev /tmp
```

Or

Edit `/etc/systemd/system/local-fs.target.wants/tmp.mount` to add `nodev` to the `/tmp` mount options:

```
[Mount]
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to remount `/tmp`:

```
# mount -o remount,nodev /tmp
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230511

Rule ID: SV-230511r627750_rule

STIG ID: RHEL-08-040123

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.4 Ensure nosuid option set on /tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Since the `/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot create `setuid` files in `/tmp`.

Audit:

Verify that the `nosuid` option is set if a `/tmp` partition exists

Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/tmp\s' | grep -v nosuid
```

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/tmp` partition. See the `fstab(5)` manual page for more information.

Run the following command to remount `/tmp`:

```
# mount -o remount,nosuid /tmp
```

Or

Edit `/etc/systemd/system/local-fs.target.wants/tmp.mount` to add `nosuid` to the `/tmp` mount options:

```
[Mount]
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to remount `/tmp`:

```
# mount -o remount,nosuid /tmp
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230512

Rule ID: SV-230512r627750_rule

STIG ID: RHEL-08-040124

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.5 Ensure noexec option set on /tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Since the `/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from `/tmp`.

Audit:

Verify that the `noexec` option is set if a `/tmp` partition exists

Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/tmp\s' | grep -v noexec
```

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/tmp` partition. See the `fstab(5)` manual page for more information.

Run the following command to remount `/tmp`:

```
# mount -o remount,noexec /tmp
```

Or

Edit `/etc/systemd/system/local-fs.target.wants/tmp.mount` to add `noexec` to the `/tmp` mount options:

```
[Mount]
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to remount `/tmp`:

```
# mount -o remount,noexec /tmp
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230513

Rule ID: SV-230513r627750_rule

STIG ID: RHEL-08-040125

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

1.1.6 Ensure separate partition exists for /var (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

Description:

The `/var` directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable.

Rationale:

Since the `/var` directory may contain world-writable files and directories, there is a risk of resource exhaustion if it is not bound to a separate partition.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Audit:

Run the following command and verify output shows `/var` is mounted:

```
# mount | grep -E '\s/var\s'  
/dev/xvdd1 on /var type xfs (rw,relatime,data=ordered)
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var`.

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>

Additional Information:

When modifying `/var` it is advisable to bring the system to emergency mode (so `audited` is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multiuser mode.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide
Version 1, Release: 3 Benchmark Date: 23 Jul 2021
Vul ID: V-230292
Rule ID: SV-230292r627750_rule
STIG ID: RHEL-08-010540
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.7 Ensure separate partition exists for /var/tmp (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

Description:

The `/var/tmp` directory is a world-writable directory used for temporary storage by all users and some applications.

Rationale:

Since the `/var/tmp` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition. In addition, making `/var/tmp` its own file system allows an administrator to set the `noexec` option on the mount, making `/var/tmp` useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system `setuid` program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Audit:

Run the following command and verify output shows `/var/tmp` is mounted:

```
# mount | grep /var/tmp  
<device> on /var/tmp type xfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/tmp`.

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244529

Rule ID: SV-244529r743836_rule

STIG ID: RHEL-08-010544

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.8 Ensure nodev option set on /var/tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/var/tmp` filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices in `/var/tmp`.

Audit:

Verify that the `nodev` option is set if a `/var/tmp` partition exists.
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/var/tmp\s' | grep -v nodev
```

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var/tmp` partition. See the `fstab(5)` manual page for more information.

Run the following command to remount `/var/tmp`:

```
# mount -o remount,nodev /var/tmp
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230520

Rule ID: SV-230520r627750_rule

STIG ID: RHEL-08-040132

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>			
v8	<p>4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v7	<p>5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			

1.1.9 Ensure nosuid option set on /var/tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Since the `/var/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot create `setuid` files in `/var/tmp`.

Audit:

Verify that the `nosuid` option is set if a `/var/tmp` partition exists.

Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/var/tmp\s' | grep -v nosuid
```

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var/tmp` partition. See the `fstab(5)` manual page for more information.

Run the following command to remount `/var/tmp`:

```
# mount -o remount,nosuid /var/tmp
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230521

Rule ID: SV-230521r627750_rule

STIG ID: RHEL-08-040133

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists</p> <p>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v8	<p>4.1 Establish and Maintain a Secure Configuration Process</p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v7	<p>5.1 Establish Secure Configurations</p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>	●	●	●

1.1.10 Ensure noexec option set on /var/tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Since the `/var/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from `/var/tmp`.

Audit:

Verify that the `noexec` option is set if a `/var/tmp` partition exists.

Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/var/tmp\s' | grep -v noexec
```

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var/tmp` partition. See the `fstab(5)` manual page for more information.

Run the following command to remount `/var/tmp`:

```
# mount -o remount,noexec /var/tmp
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230522

Rule ID: SV-230522r627750_rule

STIG ID: RHEL-08-040134

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.</p>			
v7	<p>2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner</p>			

1.1.11 Ensure separate partition exists for /var/log (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

Description:

The `/var/log` directory is used by system services to store log data .

Rationale:

There are two important reasons to ensure that system logs are stored on a separate partition: protection against resource exhaustion (since logs can grow quite large) and protection of audit data.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Audit:

Run the following command and verify output shows `/var/log` is mounted:

```
# mount | grep /var/log  
/dev/xvdh1 on /var/log type xfs (rw,relatime,data=ordered)
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/log` .

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>

Additional Information:

When modifying `/var/log` it is advisable to bring the system to emergency mode (so `auditd` is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multiuser mode.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide
Version 1, Release: 3 Benchmark Date: 23 Jul 2021
Vul ID: V-230293
Rule ID: SV-230293r627750_rule
STIG ID: RHEL-08-010541
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.	●	●	●

1.1.12 Ensure separate partition exists for /var/log/audit (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

Description:

The auditing daemon, `auditd`, stores log data in the `/var/log/audit` directory.

Rationale:

There are two important reasons to ensure that data gathered by `auditd` is stored on a separate partition: protection against resource exhaustion (since the `audit.log` file can grow quite large) and protection of audit data. The audit daemon calculates how much free space is left and performs actions based on the results. If other processes (such as `syslog`) consume space in the same partition as `auditd`, it may not perform as desired.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Audit:

Run the following command and verify output shows `/var/log/audit` is mounted:

```
# mount | grep /var/log/audit  
/dev/xvdi1 on /var/log/audit type xfs (rw,relatime,data=ordered)
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/log/audit`.

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>

Additional Information:

When modifying `/var/log/audit` it is advisable to bring the system to emergency mode (so `auditd` is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multiuser mode.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide
Version 1, Release: 3 Benchmark Date: 23 Jul 2021
Vul ID: V-230294
Rule ID: SV-230294r627750_rule
STIG ID: RHEL-08-010542
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

1.1.13 Ensure separate partition exists for /home (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `/home` directory is used to support disk storage needs of local users.

Rationale:

If the system is intended to support local users, create a separate partition for the `/home` directory to protect against resource exhaustion and restrict the type of files that can be stored under `/home`.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Audit:

Run the following command and verify output shows `/home` is mounted:

```
# mount | grep /home  
  
/dev/xvdf1 on /home type xfs (rw, nodev, relatime, data=ordered)
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/home`.

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.14 Ensure nodev option set on /home partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the user partitions are not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices.

Audit:

Verify that the `nodev` option is set if a `/home` partition exists.

Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/home\s' | grep -v nodev
```

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/home` partition. See the `fstab(5)` manual page for more information.

```
# mount -o remount,nodev /home
```

Additional Information:

The actions in this recommendation refer to the `/home` partition, which is the default user partition that is defined in many distributions. If you have created other user partitions, it is recommended that the Remediation and Audit steps be applied to these partitions as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.15 Ensure nodev option set on /dev/shm partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/dev/shm` filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create special devices in `/dev/shm` partitions.

Audit:

Verify that the `nodev` option is set if a `/dev/shm` partition exists.
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/dev/shm\s' | grep -v nodev
```

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/dev/shm` partition. See the `fstab(5)` manual page for more information.

Run the following command to remount `/dev/shm`:

```
# mount -o remount,nodev /dev/shm
```

Additional Information:

Some distributions mount `/dev/shm` through other means and require `/dev/shm` to be added to `/etc/fstab` even though it is already being mounted on boot. Others may configure `/dev/shm` in other locations and may override `/etc/fstab` configuration. Consult the documentation appropriate for your distribution.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide
Version 1, Release: 3 Benchmark Date: 23 Jul 2021
Vul ID: V-230508
Rule ID: SV-230508r627750_rule
STIG ID: RHEL-08-040120
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.16 Ensure nosuid option set on /dev/shm partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

Audit:

Verify that the `nosuid` option is set if a `/dev/shm` partition exists.

Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/dev/shm\s' | grep -v nosuid
```

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/dev/shm` partition. See the `fstab(5)` manual page for more information.

Run the following command to remount `/dev/shm`:

```
# mount -o remount,nosuid /dev/shm
```

Additional Information:

Some distributions mount `/dev/shm` through other means and require `/dev/shm` to be added to `/etc/fstab` even though it is already being mounted on boot. Others may configure `/dev/shm` in other locations and may override `/etc/fstab` configuration. Consult the documentation appropriate for your distribution.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide
Version 1, Release: 3 Benchmark Date: 23 Jul 2021
Vul ID: V-230509
Rule ID: SV-230509r627750_rule
STIG ID: RHEL-08-040121
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.17 Ensure noexec option set on /dev/shm partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Setting this option on a file system prevents users from executing programs from shared memory. This deters users from introducing potentially malicious software on the system.

Audit:

Verify that the `noexec` option is set if a `/dev/shm` partition exists.

Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/dev/shm\s' | grep -v noexec
```

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/dev/shm` partition. See the `fstab(5)` manual page for more information.

Run the following command to remount `/dev/shm`:

```
# mount -o remount,noexec /dev/shm
```

Additional Information:

Some distributions mount `/dev/shm` through other means and require `/dev/shm` to be added to `/etc/fstab` even though it is already being mounted on boot. Others may configure `/dev/shm` in other locations and may override `/etc/fstab` configuration. Consult the documentation appropriate for your distribution.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230510

Rule ID: SV-230510r627750_rule

STIG ID: RHEL-08-040122

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

1.1.18 Ensure nodev option set on removable media partitions (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Removable media containing character and block special devices could be used to circumvent security controls by allowing non-root users to access sensitive device files such as `/dev/kmem` or the raw disk partitions.

Audit:

Run the following command and verify that the `nodev` option is set on all removable media partitions.

```
# mount
```

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) of all removable media partitions. Look for entries that have mount points that contain words such as floppy or cdrom. See the `fstab(5)` manual page for more information.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230303

Rule ID: SV-230303r627750_rule

STIG ID: RHEL-08-010600

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>			
v8	<p>4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v7	<p>5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>			

1.1.19 Ensure nosuid option set on removable media partitions (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

Audit:

Run the following command and verify that the `nosuid` option is set on all removable media partitions.

```
# mount
```

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) of all removable media partitions. Look for entries that have mount points that contain words such as floppy or cdrom. See the `fstab(5)` manual page for more information.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230305

Rule ID: SV-230305r627750_rule

STIG ID: RHEL-08-010620

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.20 Ensure noexec option set on removable media partitions (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Setting this option on a file system prevents users from executing programs from the removable media. This deters users from being able to introduce potentially malicious software on the system.

Audit:

Run the following command and verify that the `noexec` option is set on all removable media partitions.

```
# mount
```

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) of all removable media partitions. Look for entries that have mount points that contain words such as floppy or cdrom. See the `fstab(5)` manual page for more information.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230304

Rule ID: SV-230304r627750_rule

STIG ID: RHEL-08-010610

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

1.1.21 Ensure sticky bit is set on all world-writable directories (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them.

Rationale:

This feature prevents the ability to delete or rename files in world writable directories (such as `/tmp`) that are owned by another user.

Audit:

Run the following command to verify no world writable directories exist without the sticky bit set:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \|) 2>/dev/null
```

No output should be returned.

Remediation:

Run the following command to set the sticky bit on all world writable directories:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \|) 2>/dev/null | xargs -I '{}' chmod a+t '{}'
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230243

Rule ID: SV-230243r627750_rule

STIG ID: RHEL-08-010190

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.22 Disable Automounting (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation
- STIG

Description:

`autofs` allows automatic mounting of devices, typically including CD/DVDs and USB drives.

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

Impact:

The use of portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

Audit:

Run the following command to verify `autofs` is not enabled:

```
# systemctl is-enabled autofs  
disabled
```

Verify result is not "enabled".

Remediation:

Run the following command to disable `autofs`:

```
# systemctl --now disable autofs
```

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

This control should align with the tolerance of the use of portable drives and optical media in the organization. On a server requiring an admin to manually mount media can be part of defense-in-depth to reduce the risk of unapproved software or information being introduced or proprietary software or information being exfiltrated. If admins commonly use flash drives and Server access has sufficient physical controls, requiring manual mounting may not increase security.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide
Version 1, Release: 3 Benchmark Date: 23 Jul 2021
Vul ID: V-230502
Rule ID: SV-230502r627750_rule
STIG ID: RHEL-08-040070
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.4 Configure Anti-Malware Scanning of Removable Devices Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

1.1.23 Disable USB Storage (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

USB storage provides a means to transfer and store files insuring persistence and availability of the files independent of network connection status. Its popularity and utility have led to USB-based malware being a simple and common means for network infiltration and a first step to establishing a persistent threat within a networked environment.

Rationale:

Restricting USB access on the system will decrease the physical attack surface for a device and diminish the possible vectors to introduce malware.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v usb-storage  
  
install /bin/true  
  
# lsmod | grep usb-storage  
  
<No output>
```

Remediation:

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf

Example: vim /etc/modprobe.d/usb_storage.conf
and add the following line:

```
install usb-storage /bin/true
```

Run the following command to unload the usb-storage module:

```
rmmmod usb-storage
```

Additional Information:

An alternative solution to disabling the usb-storage module may be found in USBGuard.

Use of USBGuard and construction of USB device policies should be done in alignment with site policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	8.4 Configure Anti-Malware Scanning of Removable Devices Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

1.1.24 Ensure file systems that contain user home directories are mounted with the "nosuid" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent files with the setuid and setgid bit set from being executed on file systems that contain user home directories.

Rationale:

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setgid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify file systems that contain user home directories are mounted with the "nosuid" option.

Note: If a separate file system has not been created for the user home directories (user home directories are mounted under "/"), this is automatically a finding as the "nosuid" option cannot be used on the "/" system.

Find the file system(s) that contain the user home directories with the following command:

```
# awk -F: '($3>=1000)&&($7 !~ /nologin/){print $1,$3,$6}' /etc/passwd
smithj:1001: /home smithj
robinst:1002: /home robinst
```

Check the file systems that are mounted at boot time with the following command:

```
# more /etc/fstab
UUID=a411dc99-f2a1-4c87-9e05-184977be8539 /home xfs
rw,relatime,discard,data=ordered,nosuid,nodev,noexec 0 0
```

If a file system found in "/etc/fstab" refers to the user home directory file system and it does not have the "nosuid" option set, this is a finding.

Remediation:

Configure "/etc/fstab" to use the "nosuid" option on file systems that contain user home directories for interactive users.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230299

Rule ID: SV-230299r627750_rule

STIG ID: RHEL-08-010570

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.25 Ensure the "/boot" directory is mounted with the "nosuid" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent files with the "setuid" and "setgid" bit set from being executed on the "/boot" directory.

Rationale:

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setgid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

For systems that use UEFI, this is Not Applicable.

Verify the /boot directory is mounted with the "nosuid" option with the following command:

```
# mount | grep '\s/boot\s'  
/dev/sda1 on /boot type xfs  
(rw,nosuid,relatime,seclabe,attr2,inode64,noquota)
```

If the "/boot" file system does not have the "nosuid" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nosuid" option on the /boot directory.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230300

Rule ID: SV-230300r743959_rule

STIG ID: RHEL-08-010571

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.26 Ensure all non-root local partitions are mounted with the "nodev" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent special devices on non-root local partitions.

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access. The only legitimate location for device files is the "/dev" directory located on the root partition.

Audit:

Verify all non-root local partitions are mounted with the "nodev" option with the following command:

```
# mount | grep '^/dev\S*' | grep --invert-match 'nodev'
```

If any output is produced, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nodev" option on all non-root local partitions.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230301

Rule ID: SV-230301r627750_rule

STIG ID: RHEL-08-010580

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.27 Ensure file systems that are being NFS-imported are mounted with the "nodev" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent special devices on file systems that are imported via Network File System (NFS).

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify file systems that are being NFS-imported are mounted with the "nodev" option with the following command:

```
# grep nfs /etc/fstab | grep nodev  
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid,nodev,noexec 0 0
```

If a file system found in "/etc/fstab" refers to NFS and it does not have the "nodev" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nodev" option on file systems that are being imported via NFS.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230307

Rule ID: SV-230307r627750_rule

STIG ID: RHEL-08-010640

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.28 Ensure file systems being imported via NFS are mounted with the "noexec" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent code from being executed on file systems that are imported via Network File System (NFS).

Rationale:

The "noexec" mount option causes the system not to execute binary files. This option must be used for mounting any file system not containing approved binary as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify that file systems being imported via NFS are mounted with the "noexec" option with the following command:

```
# grep nfs /etc/fstab | grep noexec  
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid,nodev,noexec 0
```

If a file system found in "/etc/fstab" refers to NFS and it does not have the "noexec" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "noexec" option on file systems that are being imported via NFS.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230306

Rule ID: SV-230306r627750_rule

STIG ID: RHEL-08-010630

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.29 Ensure file systems being imported via NFS are mounted with the "nosuid" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent files with the setuid and setgid bit set from being executed on file systems that are imported via Network File System (NFS).

Rationale:

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setgid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify that file systems being imported via NFS are mounted with the "nosuid" option with the following command:

```
# grep nfs /etc/fstab | grep nosuid  
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid,nodev,noexec 0 0
```

If a file system found in "/etc/fstab" refers to NFS and it does not have the "nosuid" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nosuid" option on file systems that are being imported via NFS.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230308

Rule ID: SV-230308r627750_rule

STIG ID: RHEL-08-010650

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.30 Ensure a separate file system/partition has been created for non-privileged local interactive user home directories (Automated)

Profile Applicability:

- STIG

Description:

A separate filesystem must be used for user home directories (such as /home or an equivalent).

Rationale:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Audit:

Verify that a separate file system/partition has been created for non-privileged local interactive user home directories.

Check the home directory assignment for all non-privileged users, users with a User Identifier (UID) greater than 1000, on the system with the following command:

```
# awk -F: '($3>=1000) && ($7 !~ /nologin/) {print $1,$3,$6}' /etc/passwd
adamsj 1001 /home/adamsj
jacksonm 1002 /home/jacksonm
smithj 1003 /home smithj
```

The output of the command will give the directory/partition that contains the home directories for the non-privileged users on the system (in this example, "/home") and users' shell. All accounts with a valid shell (such as /bin/bash) are considered interactive users.

Check that a file system/partition has been created for the non-privileged interactive users with the following command:

Note: The partition of "/home" is used in the example.

```
# grep /home /etc/fstab
UUID=333ada18 /home ext4 noatime,nobarrier,nodev 1 2
```

If a separate entry for the file system/partition containing the non-privileged interactive user home directories does not exist, this is a finding.

Remediation:

Migrate the "/home" directory onto a separate file system/partition.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide
Version 1, Release: 3 Benchmark Date: 23 Jul 2021
Vul ID: V-230328
Rule ID: SV-230328r627750_rule
STIG ID: RHEL-08-010800
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.31 Ensure "/var/log" is mounted with the "nodev" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must mount "/var/log" with the "nodev" option.

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log" is mounted with the "nodev" option:

```
# mount | grep /var/log
/dev/mapper/rhel-var-log on /var/log type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nodev" option is configured for "/var/log":

```
# cat /etc/fstab | grep /var/log
/dev/mapper/rhel-var-log /var/log xfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "nodev" option is missing, or if "/var/log" is mounted without the "nodev" option, this is a finding.

Remediation:

Configure the system so that "/var/log" is mounted with the "nodev" option by adding/modifying the "/etc/fstab" with the following line:

```
/dev/mapper/rhel-var-log /var/log xfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230514

Rule ID: SV-230514r627750_rule

STIG ID: RHEL-08-040126

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

1.1.32 Ensure "/var/log" is mounted with the "nosuid" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must mount "/var/log" with the "nosuid" option.

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setgid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log" is mounted with the "nosuid" option:

```
# mount | grep /var/log
/dev/mapper/rhel-var-log on /var/log type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nosuid" option is configured for "/var/log":

```
# cat /etc/fstab | grep /var/log
/dev/mapper/rhel-var-log /var/log xfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "nosuid" option is missing, or if "/var/log" is mounted without the "nosuid" option, this is a finding.

Remediation:

Configure the system so that "/var/log" is mounted with the "nosuid" option by adding/modifying the "/etc/fstab" with the following line:

```
/dev/mapper/rhel-var-log /var/log xfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230515

Rule ID: SV-230515r627750_rule

STIG ID: RHEL-08-040127

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

1.1.33 Ensure "/var/log" is mounted with the "noexec" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must mount "/var/log" with the "noexec" option.

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log" is mounted with the "noexec" option:

```
# mount | grep /var/log
/dev/mapper/rhel-var-log on /var/log type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "noexec" option is configured for "/var/log":

```
# cat /etc/fstab | grep /var/log
/dev/mapper/rhel-var-log /var/log xfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "noexec" option is missing, or if "/var/log" is mounted without the "noexec" option, this is a finding.

Remediation:

Configure the system so that "/var/log" is mounted with the "noexec" option by adding/modifying the "/etc/fstab" with the following line:

```
/dev/mapper/rhel-var-log /var/log xfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230516

Rule ID: SV-230516r627750_rule

STIG ID: RHEL-08-040128

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

1.1.34 Ensure "/var/log/audit" is mounted with the "nodev" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must mount "/var/log/audit" with the "nodev" option.

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log/audit" is mounted with the "nodev" option:

```
# mount | grep /var/log/audit  
  
/dev/mapper/rhel-var-log-audit on /var/log/audit type xfs  
(rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nodev" option is configured for "/var/log/audit":

```
# cat /etc/fstab | grep /var/log/audit  
  
/dev/mapper/rhel-var-log-audit /var/log/audit xfs  
defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "nodev" option is missing, or if "/var/log/audit" is mounted without the "nodev" option, this is a finding.

Remediation:

Configure the system so that "/var/log/audit" is mounted with the "nodev" option by adding/modifying the "/etc/fstab" with the following line:

```
/dev/mapper/rhel-var-log-audit /var/log/audit xfs  
defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230517

Rule ID: SV-230517r627750_rule

STIG ID: RHEL-08-040129

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

1.1.35 Ensure "/var/log/audit" is mounted with the "nosuid" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must mount "/var/log/audit" with the "nosuid" option.

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log/audit" is mounted with the "nosuid" option:

```
# mount | grep /var/log/audit  
  
/dev/mapper/rhel-var-log-audit on /var/log/audit type xfs  
(rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nosuid" option is configured for "/var/log/audit":

```
# cat /etc/fstab | grep /var/log/audit  
  
/dev/mapper/rhel-var-log-audit /var/log/audit xfs  
defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "nosuid" option is missing, or if "/var/log/audit" is mounted without the "nosuid" option, this is a finding.

Remediation:

Configure the system so that "/var/log/audit" is mounted with the "nosuid" option by adding/modifying the "/etc/fstab" with the following line:

```
/dev/mapper/rhel-var-log-audit /var/log/audit xfs  
defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230518

Rule ID: SV-230518r627750_rule

STIG ID: RHEL-08-040130

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

1.1.36 Ensure "/var/log/audit" is mounted with the "noexec" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must mount "/var/log/audit" with the "noexec" option.

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log/audit" is mounted with the "noexec" option:

```
# mount | grep /var/log/audit  
  
/dev/mapper/rhel-var-log-audit on /var/log/audit type xfs  
(rw,nosuid,noexec,seclabel)
```

Verify that the "noexec" option is configured for "/var/log/audit":

```
# cat /etc/fstab | grep /var/log/audit  
  
/dev/mapper/rhel-var-log-audit /var/log/audit xfs  
defaults,nosuid,noexec 0 0
```

If results are returned and the "noexec" option is missing, or if "/var/log/audit" is mounted without the "noexec" option, this is a finding.

Remediation:

Configure the system so that "/var/log/audit" is mounted with the "noexec" option by adding/modifying the "/etc/fstab" with the following line:

```
/dev/mapper/rhel-var-log-audit /var/log/audit xfs  
defaults,nosuid,noexec 0 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230519

Rule ID: SV-230519r627750_rule

STIG ID: RHEL-08-040131

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

1.1.37 Ensure the "/boot/efi" directory is mounted with the "nosuid" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent files with the "setuid" and "setgid" bit set from being executed on the "/boot/efi" directory.

Rationale:

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setgid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

For systems that use BIOS, this is Not Applicable.

Verify the "/boot/efi" directory is mounted with the "nosuid" option with the following command:

```
# mount | grep '\s/boot/efi\s'  
/dev/sda1 on /boot/efi type xfs  
(rw,nosuid,relatime,seclabe,attr2,inode64,noquota)
```

If the "/boot/efi" file system does not have the "nosuid" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nosuid" option on the "/boot/efi" directory.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244530

Rule ID: SV-244530r743839_rule

STIG ID: RHEL-08-010572

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.38 Ensure file systems that contain user home directories are mounted with the "noexec" option (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent code from being executed on file systems that contain user home directories.

Rationale:

The "noexec" mount option causes the system not to execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify file systems that contain user home directories are mounted with the "noexec" option.

Note: If a separate file system has not been created for the user home directories (user home directories are mounted under "/"), this is automatically a finding as the "noexec" option cannot be used on the "/" system.

Find the file system(s) that contain the user home directories with the following command:

```
# awk -F: '($3>=1000)&&($7 !~ /nologin/){print $1,$3,$6}' /etc/passwd
smithj:1001: /home smithj
robinst:1002: /home robinst
```

Check the file systems that are mounted at boot time with the following command:

```
# more /etc/fstab
UUID=a411dc99-f2a1-4c87-9e05-184977be8539 /home ext4
rw,relatime,discard,data=ordered,nosuid,nodev,noexec 0 2
```

If a file system found in "/etc/fstab" refers to the user home directory file system and it does not have the "noexec" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "noexec" option on file systems that contain user home directories for interactive users.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230302

Rule ID: SV-230302r627750_rule

STIG ID: RHEL-08-010590

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.2 Configure Software Updates

Fedora 28 derived Linux distributions use dnf (previously yum) to install and update software packages. Patch management procedures may vary widely between enterprises.

Large enterprises may choose to install a local updates server that can be used in place of their distributions servers, whereas a single deployment of a system may prefer to get updates directly. Updates can be performed automatically or manually, depending on the site's policy for patch management. Many large enterprises prefer to test patches on a non-production system before rolling out to production.

For the purpose of this benchmark, the requirement is to ensure that a patch management system is configured and maintained. The specifics on patch update procedures are left to the organization.

1.2.1 Ensure GPG keys are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Most packages managers implement GPG key signing to verify package integrity during installation.

Rationale:

It is important to ensure that updates are obtained from a valid source to protect against spoofing that could lead to the inadvertent installation of malware on the system.

Audit:

Verify GPG keys are configured correctly for your package manager. Depending on the package management in use one of the following command groups may provide the needed information:

```
# rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'
```

Remediation:

Update your package manager GPG keys in accordance with site policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	<u>7.4 Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

1.2.2 Ensure gpgcheck is globally activated (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `gpgcheck` option, found in the main section of the `/etc/yum.conf` and individual `/etc/yum/repos.d/*` files determines if an RPM package's signature is checked prior to its installation.

Rationale:

It is important to ensure that an RPM's package signature is always checked prior to installation to ensure that the software is obtained from a trusted source.

Audit:

Run the following command and verify `gpgcheck` is set to '1':

```
# grep ^gpgcheck /etc/yum.conf  
gpgcheck=1
```

Run the following command and verify that all instances of `gpgcheck` returned are set to '1':

```
# grep ^gpgcheck /etc/yum.repos.d/*
```

Remediation:

Edit `/etc/yum.conf` and set '`gpgcheck=1`' in the `[main]` section.

Edit any failing files in `/etc/yum.repos.d/*` and set all instances of `gpgcheck` to '1'.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230264

Rule ID: SV-230264r627750_rule

STIG ID: RHEL-08-010370

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

1.2.3 Ensure package manager repositories are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Systems need to have package manager repositories configured to ensure they receive the latest patches and updates.

Rationale:

If a system's package repositories are misconfigured important patches may not be identified or a rogue repository could introduce compromised software.

Audit:

Run the following command to verify repositories are configured correctly:

```
# dnf repolist
```

Remediation:

Configure your package manager repositories according to site policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

1.2.4 Ensure DNF is configured to perform a signature check on local packages (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

Rationale:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Audit:

Verify the operating system prevents the installation of patches, service packs, device drivers, or operating system components from a repository without verification that they have been digitally signed using a certificate that is recognized and approved by the organization.

Check if DNF is configured to perform a signature check on local packages with the following command:

```
# grep -i localpkg_gpgcheck /etc/dnf/dnf.conf  
localpkg_gpgcheck =True
```

If "localpkg_gpgcheck" is not set to either "1", "True", or "yes", commented out, or is missing from "/etc/dnf/dnf.conf", this is a finding.

Remediation:

Configure the operating system to remove all software components after updated versions have been installed.

Set the "localpkg_gpgcheck" option to "True" in the "/etc/dnf/dnf.conf" file:

```
localpkg_gpgcheck=True
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230265

Rule ID: SV-230265r627750_rule

STIG ID: RHEL-08-010371

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

1.3 Configure sudo

sudo allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

sudo supports a plugin architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plugins to work seamlessly with the sudo front end. The default security policy is sudoers, which is configured via the file /etc/sudoers.

1.3.1 Ensure sudo is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

Rationale:

sudo supports a plugin architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plugins to work seamlessly with the sudo front end. The default security policy is sudoers, which is configured via the file /etc/sudoers.

The security policy determines what privileges, if any, a user has to run sudo. The policy may require that users authenticate themselves with a password or another authentication mechanism. If authentication is required, sudo will exit if the user's password is not entered within a configurable time limit. This limit is policy-specific.

Audit:

Verify that sudo is installed.

Run the following command:

```
# rpm -q sudo  
sudo-<VERSION>
```

Remediation:

Run the following command to install sudo

```
# dnf install sudo
```

References:

1. SUDO(8)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v7	<p>4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.</p>	●	●	●

1.3.2 Ensure sudo commands use pty (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo can be configured to run only from a psuedo-pty

Rationale:

Attackers can run a malicious program using sudo which would fork a background process that remains even when the main program has finished executing.

Impact:

editing the sudo configuration incorrectly can cause sudo to stop functioning.

Audit:

Verify that sudo can only run other commands from a psuedo-pty

Run the following command:

```
# grep -Ei '^s*Defaults\s+(\[^#]+,\s*)?use_pty' /etc/sudoers  
/etc/sudoers.d/*  
  
Defaults use_pty
```

Remediation:

edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo -f` and add the following line:

```
Defaults use_pty
```

References:

1. SUDO(8)
2. VISUDO(8)

Additional Information:

visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks or parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.3.3 Ensure sudo log file exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo can use a custom log file

Rationale:

A sudo log file simplifies auditing of sudo commands

Impact:

editing the sudo configuration incorrectly can cause sudo to stop functioning

Audit:

Run the following command to verify that sudo has a custom log file configured

```
# grep -Esi '^s*Defaults\s+([^\#]+\s*)?logfile=' /etc/sudoers  
/etc/sudoers.d/*  
  
Defaults logfile="/var/log/sudo.log"
```

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo` or `visudo -f` and add the following line:

```
Defaults    logfile=<PATH TO CUSTOM LOG FILE>"
```

Example

```
Defaults logfile="/var/log/sudo.log"
```

References:

1. SUDO(8)
2. VISUDO(8)

Additional Information:

visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

1.3.4 Ensure the "/etc/sudoers" file has no occurrences of "NOPASSWD" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must require users to provide a password for privilege escalation.

Rationale:

Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Audit:

Verify that "/etc/sudoers" has no occurrences of "NOPASSWD".

Check that the "/etc/sudoers" file has no occurrences of "NOPASSWD" by running the following command:

```
# grep -i nopasswd /etc/sudoers /etc/sudoers.d/*  
%admin ALL=(ALL) NOPASSWD: ALL
```

If any occurrences of "NOPASSWD" are returned from the command and have not been documented with the ISSO as an organizationally defined administrative group utilizing MFA, this is a finding.

Remediation:

Remove any occurrence of "NOPASSWD" found in "/etc/sudoers" file or files in the "/etc/sudoers.d" directory.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230271

Rule ID: SV-230271r627750_rule

STIG ID: RHEL-08-010380

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

1.3.5 Ensure the "/etc/sudoers" file has no occurrences of "!authenticate" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must require users to reauthenticate for privilege escalation.

Rationale:

Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Audit:

Verify that "/etc/sudoers" has no occurrences of "!authenticate".

Check that the "/etc/sudoers" file has no occurrences of "!authenticate" by running the following command:

```
# grep -i !authenticate /etc/sudoers /etc/sudoers.d/*
```

If any occurrences of "!authenticate" return from the command, this is a finding.

Remediation:

Remove any occurrence of "!authenticate" found in "/etc/sudoers" file or files in the "/etc/sudoers.d" directory.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230272

Rule ID: SV-230272r627750_rule

STIG ID: RHEL-08-010381

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

1.3.6 Ensure the "sudoers" file restricts sudo access to authorized personnel (Automated)

Profile Applicability:

- STIG

Description:

The operating system must restrict privilege elevation to authorized personnel.

Rationale:

The sudo command allows a user to execute programs with elevated (administrator) privileges. It prompts the user for their password and confirms your request to execute a command by checking a file, called sudoers. If the "sudoers" file is not configured correctly, any user defined on the system can initiate privileged actions on the target system.

Audit:

Verify the "sudoers" file restricts sudo access to authorized personnel:

```
# grep -iw 'ALL' /etc/sudoers /etc/sudoers.d/*
```

If either of the following entries are returned, this is a finding:

```
ALL ALL=(ALL) ALL
ALL ALL=(ALL:ALL) ALL
```

Remediation:

Remove the following entries from the sudoers file:

```
ALL ALL=(ALL) ALL
ALL ALL=(ALL:ALL) ALL
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-237641

Rule ID: SV-237641r646893_rule

STIG ID: RHEL-08-010382

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	<u>5.4 Deploy System Configuration Management Tools</u> Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

1.3.7 Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation (Automated)

Profile Applicability:

- STIG

Description:

The operating system must use the invoking user's password for privilege escalation when using "sudo".

Rationale:

The sudoers security policy requires that users authenticate themselves before they can use sudo. When sudoers requires authentication, it validates the invoking user's credentials. If the rootpw, targetpw, or runaspw flags are defined and not disabled, by default the operating system will prompt the invoking user for the "root" user password.

For more information on each of the listed configurations, reference the sudoers(5) manual page.

Audit:

Verify that the sudoers security policy is configured to use the invoking user's password for privilege escalation.

```
# grep -E '(!rootpw|!targetpw|!runaspw)' /etc/sudoers /etc/sudoers.d/* | grep -v '#'  
  
/etc/sudoers:Defaults !targetpw  
/etc/sudoers:Defaults !rootpw  
/etc/sudoers:Defaults !runaspw
```

If no results are returned, this is a finding.

If "Defaults !targetpw" is not defined, this is a finding.

If "Defaults !rootpw" is not defined, this is a finding.

If "Defaults !runaspw" is not defined, this is a finding.

Remediation:

Define the following in the Defaults section of the /etc/sudoers file or a configuration file in the /etc/sudoers.d/ directory:

```
Defaults !targetpw  
Defaults !rootpw  
Defaults !runaspw
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-237642

Rule ID: SV-237642r646896_rule

STIG ID: RHEL-08-010383

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

1.3.8 Ensure the operating system requires re-authentication when using the "sudo" command to elevate privileges (Automated)

Profile Applicability:

- STIG

Description:

The operating system must require re-authentication when using the "sudo" command.

Rationale:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the organization requires the user to re-authenticate when using the "sudo" command.

If the value is set to an integer less than 0, the user's time stamp will not expire and the user will not have to re-authenticate for privileged actions until the user's session is terminated.

Audit:

Verify the operating system requires re-authentication when using the "sudo" command to elevate privileges.

```
# grep -i 'timestamp_timeout' /etc/sudoers /etc/sudoers.d/*
/etc/sudoers:Defaults timestamp_timeout=0
```

If "timestamp_timeout" is set to a negative number, is commented out, or no results are returned, this is a finding.

Remediation:

Configure the "sudo" command to require re-authentication.

Edit the /etc/sudoers file:

```
# visudo
```

Add or modify the following line:

```
Defaults timestamp_timeout=[value]
```

Note: The "[value]" must be a number that is greater than or equal to "0".

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-237643

Rule ID: SV-237643r646899_rule

STIG ID: RHEL-08-010384

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	<u>5.4 Deploy System Configuration Management Tools</u> Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

1.4 Filesystem Integrity Checking

AIDE is a file integrity checking tool, similar in nature to Tripwire. While it cannot prevent intrusions, it can detect unauthorized changes to configuration files by alerting when the files are changed. When setting up AIDE, decide internally what the site policy will be concerning integrity checking. Review the AIDE quick start guide and AIDE documentation before proceeding.

1.4.1 Ensure AIDE is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

AIDE takes a snapshot of filesystem state including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system.

Rationale:

By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

Audit:

Run the following command and verify `aide` is installed:

```
# rpm -q aide  
aide-<version>
```

Remediation:

Run the following command to install AIDE:

```
# dnf install aide
```

Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options.

Initialize AIDE:

Run the following commands:

```
# aide --init  
# mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

References:

1. AIDE stable manual: <http://aide.sourceforge.net/stable/manual.html>

Additional Information:

The prelinking feature can interfere with AIDE because it alters binaries to speed up their start up times. Run `prelink -ua` to restore the binaries to their prelinked state, thus avoiding false positives from AIDE.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

1.4.2 Ensure filesystem integrity is regularly checked (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

Periodic checking of the filesystem integrity is needed to detect changes to the filesystem.

Rationale:

Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

Audit:

Run the following commands to verify a cron job scheduled to run the aide check.

```
# grep -Ers '^([^\#]+\s+)?(/usr/s?bin/|^s*)aide(\.wrapper)?\s(--?\S+\s)*(-  
-(check|update)|\$AIDEARGS)\b' /etc/cron.* /etc/crontab /var/spool/cron/
```

Ensure a cron job in compliance with site policy is returned.

Or

Run the following commands to verify that aidecheck.service and aidecheck.timer are enabled and aidecheck.timer is running

```
# systemctl is-enabled aidecheck.service  
  
# systemctl is-enabled aidecheck.timer  
# systemctl status aidecheck.timer
```

Remediation:

If cron will be used to schedule and run aide check

Run the following command:

```
# crontab -u root -e
```

Add the following line to the crontab:

```
0 5 * * * /usr/sbin/aide --check
```

Or

If aidecheck.service and aidecheck.timer will be used to schedule and run aide check:

Create or edit the file `/etc/systemd/system/aidecheck.service` and add the following lines:

```
[Unit]
Description=Aide Check

[Service]
Type=simple
ExecStart=/usr/sbin/aide --check

[Install]
WantedBy=multi-user.target
```

Create or edit the file `/etc/systemd/system/aidecheck.timer` and add the following lines:

```
[Unit]
Description=Aide check every day at 5AM

[Timer]
OnCalendar=*-*-* 05:00:00
Unit=aidecheck.service

[Install]
WantedBy=multi-user.target
```

Run the following commands:

```
# chown root:root /etc/systemd/system/aidecheck.*
# chmod 0644 /etc/systemd/system/aidecheck.*

# systemctl daemon-reload

# systemctl enable aidecheck.service
# systemctl --now enable aidecheck.timer
```

References:

1. <https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.service>
2. <https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.timer>

Additional Information:

The checking in this recommendation occurs every day at 5am. Alter the frequency and time of the checks in compliance with site policy.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide
Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230263
Rule ID: SV-230263r627750_rule
STIG ID: RHEL-08-010360
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

1.4.3 Ensure Advanced Intrusion Detection Environment (AIDE) is properly configured to use cryptographic mechanisms to protect the integrity of audit tools (Automated)

Profile Applicability:

- STIG

Description:

The operating system must use cryptographic mechanisms to protect the integrity of audit tools.

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

It is not uncommon for attackers to replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

To address this risk, audit tools must be cryptographically signed to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Audit:

Verify that Advanced Intrusion Detection Environment (AIDE) is properly configured to use cryptographic mechanisms to protect the integrity of audit tools.

If AIDE is not installed, ask the System Administrator how file integrity checks are performed on the system.

Check the selection lines to ensure AIDE is configured to add/check with the following command:

```
# grep -E '(\ /usr\ /sbin\ /(audit|au))' /etc/aide.conf

/usr/sbin/auditctl p+i+n+u+g+s+b+acl+xattr+sha512
/usr/sbin/auditd p+i+n+u+g+s+b+acl+xattr+sha512
/usr/sbin/ausearch p+i+n+u+g+s+b+acl+xattr+sha512
/usr/sbin/aureport p+i+n+u+g+s+b+acl+xattr+sha512
/usr/sbin/autrace p+i+n+u+g+s+b+acl+xattr+sha512
/usr/sbin/rsyslogd p+i+n+u+g+s+b+acl+xattr+sha512
/usr/sbin/augenrules p+i+n+u+g+s+b+acl+xattr+sha512
```

If any of the audit tools listed above do not have an appropriate selection line, ask the system administrator to indicate what cryptographic mechanisms are being used to protect the integrity of the audit tools. If there is no evidence of integrity protection, this is a finding.

Remediation:

Add or update the following lines to "/etc/aide.conf", to protect the integrity of the audit tools.

```
# Audit Tools
/usr/sbin/auditctl p+i+n+u+g+s+b+acl+xattr+sha512
/usr/sbin/auditd p+i+n+u+g+s+b+acl+xattr+sha512
/usr/sbin/ausearch p+i+n+u+g+s+b+acl+xattr+sha512
/usr/sbin/aureport p+i+n+u+g+s+b+acl+xattr+sha512
/usr/sbin/autrace p+i+n+u+g+s+b+acl+xattr+sha512
/usr/sbin/rsyslogd p+i+n+u+g+s+b+acl+xattr+sha512
/usr/sbin/augenrules p+i+n+u+g+s+b+acl+xattr+sha512
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230475

Rule ID: SV-230475r627750_rule

STIG ID: RHEL-08-030650

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

1.4.4 Ensure the file integrity tool is configured to verify extended attributes (Manual)

Profile Applicability:

- STIG

Description:

The operating system's file integrity tool must be configured to verify extended attributes.

Rationale:

Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

Installation media come with a file integrity tool, Advanced Intrusion Detection Environment (AIDE). Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

Installation media come with a file integrity tool, Advanced Intrusion Detection Environment (AIDE).

Audit:

Verify the file integrity tool is configured to verify extended attributes.

If AIDE is not installed, ask the System Administrator how file integrity checks are performed on the system.

Note: AIDE is highly configurable at install time. This requirement assumes the "aide.conf" file is under the "/etc" directory.

Use the following command to determine if the file is in another location:

```
# find / -name aide.conf
```

Check the "aide.conf" file to determine if the "xattrs" rule has been added to the rule list being applied to the files and directories selection lists.

An example rule that includes the "xattrs" rule follows:

```
All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux  
/bin All # apply the custom rule to the files in bin  
/sbin All # apply the same custom rule to the files in sbin
```

If the "xattrs" rule is not being used on all uncommented selection lines in the "/etc/aide.conf" file, or extended attributes are not being checked by another file integrity tool, this is a finding.

Remediation:

Configure the file integrity tool to check file and directory extended attributes. If AIDE is installed, ensure the "xattrs" rule is present on all uncommented file and directory selection lists.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230551

Rule ID: SV-230551r627750_rule

STIG ID: RHEL-08-040300

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

1.4.5 Ensure the file integrity tool is configured to verify ACLs (Manual)

Profile Applicability:

- STIG

Description:

The operating system's file integrity tool must be configured to verify Access Control Lists (ACLs).

Rationale:

ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

RHEL 8 installation media come with a file integrity tool, Advanced Intrusion Detection Environment (AIDE).

Audit:

Verify the file integrity tool is configured to verify ACLs.

Note: AIDE is highly configurable at install time. This requirement assumes the "aide.conf" file is under the "/etc" directory.

If AIDE is not installed, ask the System Administrator how file integrity checks are performed on the system.

Use the following command to determine if the file is in a location other than "/etc/aide/aide.conf":

```
# find / -name aide.conf
```

Check the "aide.conf" file to determine if the "acl" rule has been added to the rule list being applied to the files and directories selection lists with the following command:

```
# grep -E "[+]?acl" /etc/aide.conf  
VarFile = OwnerMode+n+l+X+acl
```

If the "acl" rule is not being used on all selection lines in the "/etc/aide.conf" file, is commented out, or ACLs are not being checked by another file integrity tool, this is a finding.

Remediation:

Configure the file integrity tool to check file and directory ACLs.

If AIDE is installed, ensure the "acl" rule is present on all file and directory selection lists.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230552

Rule ID: SV-230552r627750_rule

STIG ID: RHEL-08-040310

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.14 Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal.			●
v7	<u>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</u> Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

1.5 Secure Boot Settings

The recommendations in this section focus on securing the bootloader and settings involved in the boot process directly.

1.5.1 Ensure permissions on bootloader config are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The grub configuration file contains information on boot settings and passwords for unlocking boot options.

The grub configuration is usually `grub.cfg` and `grubenv` stored in `/boot/grub2/`

Rationale:

Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in security upon boot and be able to exploit them.

Audit:

Run the following script to verify correct permissions, ownership, and group for grub.cfg and if it exists, user.cfg:

```
#!/bin/bash

tst1="" tst2="" tst3="" tst4="" test1="" test2="" efidir="" gbdir=""
grubdir="" grubfile="" userfile=""
efidir=$(find /boot/efi/EFI/* -type d -not -name 'BOOT')
gbdir=$(find /boot -maxdepth 1 -type d -name 'grub*')
for file in "$efidir"/grub.cfg "$efidir"/grub.conf; do
    [ -f "$file" ] && grubdir="$efidir" && grubfile=$file
done
if [ -z "$grubdir" ]; then
    for file in "$gbdir"/grub.cfg "$gbdir"/grub.conf; do
        [ -f "$file" ] && grubdir="$gbdir" && grubfile=$file
    done
fi
userfile="$grubdir/user.cfg"
stat -c "%a" "$grubfile" | grep -Pq '^h*[0-7]00$' && tst1=pass
output="Permissions on \"$grubfile\" are \"$(stat -c "%a" \"$grubfile\")\""
stat -c "%u:%g" "$grubfile" | grep -Pq '^h*0:0$' && tst2=pass
output2="\"$grubfile\" is owned by \"$(stat -c "%U" \"$grubfile\")\" and
belongs to group \"$(stat -c "%G" \"$grubfile\")\""
[ "$tst1" = pass ] && [ "$tst2" = pass ] && test1=pass
if [ -f "$userfile" ]; then
    stat -c "%a" "$userfile" | grep -Pq '^h*[0-7]00$' && tst3=pass
    output3="Permissions on \"$userfile\" are \"$(stat -c "%a" \"$userfile\")\""
    stat -c "%u:%g" "$userfile" | grep -Pq '^h*0:0$' && tst4=pass
    output4="\"$userfile\" is owned by \"$(stat -c "%U" \"$userfile\")\" and
belongs to group \"$(stat -c "%G" \"$userfile\")\""
    [ "$tst3" = pass ] && [ "$tst4" = pass ] && test2=pass
else
    test2=pass
fi
[ "$test1" = pass ] && [ "$test2" = pass ] && passing=true
# If passing is true we pass
if [ "$passing" = true ] ; then
    echo "PASSED:"
    echo "$output"
    echo "$output2"
    [ -n "$output3" ] && echo "$output3"
    [ -n "$output4" ] && echo "$output4"
else
    # print the reason why we are failing
    echo "FAILED:"
    echo "$output"
    echo "$output2"
    [ -n "$output3" ] && echo "$output3"
    [ -n "$output4" ] && echo "$output4"
fi
```

Remediation:

Run the following commands to set ownership and permissions on your grub configuration file(s):

```
# chown root:root /boot/grub2/grub.cfg
# test -f /boot/grub2/user.cfg && chown root:root /boot/grub2/user.cfg
# chmod og-rwx /boot/grub2/grub.cfg
# test -f /boot/grub2/user.cfg && chmod og-rwx /boot/grub2/user.cfg
```

OR

If the system uses UEFI, edit `/etc/fstab` and add the `fmask=0077` option:

Example:

```
<device> /boot/efi vfat defaults,umask=0027,fmask=0077,uid=0,gid=0 0 0
```

Note: This may require a re-boot to enable the change

Additional Information:

This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

Replace `/boot/grub2/grub.cfg` and `/boot/grub2/grubenv` with the appropriate configuration file(s) for your environment

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.2 Ensure bootloader password is set (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Setting the boot loader password will require that anyone rebooting the system must enter a password before being able to set command line boot parameters

Rationale:

Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off SELinux at boot time).

Impact:

If password protection is enabled, only the designated superuser can edit a Grub 2 menu item by pressing "e" or access the GRUB 2 command line by pressing "c"

If GRUB 2 is set up to boot automatically to a password-protected menu entry the user has no option to back out of the password prompt to select another menu entry. Holding the SHIFT key will not display the menu in this case. The user must enter the correct username and password. If unable, the configuration files will have to be edited via the LiveCD or other means to fix the problem

You can add --unrestricted to the menu entries to allow the system to boot without entering a password. Password will still be required to edit menu items.

Audit:

Run the following script to verify the bootloader password has been set:

```
#!/bin/bash

tst1="" tst2="" output=""
efidir=$(find /boot/efi/EFI/* -type d -not -name 'BOOT')
gbdir=$(find /boot -maxdepth 1 -type d -name 'grub*')
if [ -f "$efidir/grub.cfg" ]; then
    grubdir="$efidir" && grubfile="$efidir/grub.cfg"
elif [ -f "$gbdir/grub.cfg" ]; then
    grubdir="$gbdir" && grubfile="$gbdir/grub.cfg"
fi
userfile="$grubdir/user.cfg"
[ -f "$userfile" ] && grep -Pq '^h*GRUB2_PASSWORD\h*=\h*.+$' "$userfile" &&
output="\n PASSED: bootloader password set in \"$userfile\"\n\n"
if [ -z "$output" ] && [ -f "$grubfile" ]; then
    grep -Piq '^h*set\h+superusers\h*=\h*"?[^"\n\r]+?"(\h+.*)?$$' "$grubfile"
    && tst1=pass
    grep -Piq '^h*password\h+\H+\h+.+$' "$grubfile" && tst2=pass
    [ "$tst1" = pass ] && [ "$tst2" = pass ] && output="\n\n*** PASSED:
bootloader password set in \"$grubfile\" ***\n\n"
fi
[ -n "$output" ] && echo -e "$output" || echo -e "\n\n *** FAILED: bootloader
password is not set ***\n\n"
```

Remediation:

Create an encrypted password with `grub2-setpassword`:

```
# grub2-setpassword

Enter password: <password>
Confirm password: <password>
```

Run the following command to update the `grub2` configuration:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

Additional Information:

This recommendation is designed around the grub2 bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

Replace `/boot/grub2/grub.cfg with the appropriate grub configuration file for your environment

The superuser/user information and password do not have to be contained in the /etc/grub.d/00_header file. The information can be placed in any /etc/grub.d file as long as that file is incorporated into grub.cfg. The user may prefer to enter this data into a custom file, such as /etc/grub.d/40_custom so it is not overwritten should the Grub package be updated. If placing the information in a custom file, do not include the "cat << EOF" and "EOF" lines as the content is automatically added from these files.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.3 Ensure authentication required for single user mode (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Single user mode (rescue mode) is used for recovery when the system detects an issue during boot or by manual selection from the bootloader.

Rationale:

Requiring authentication in single user mode (rescue mode) prevents an unauthorized user from rebooting the system into single user to gain root privileges without credentials.

Audit:

Run the following commands and verify that `/sbin/sulogin` or `/usr/sbin/sulogin` is used as shown:

```
# grep /systemd-sulogin-shell /usr/lib/systemd/system/rescue.service  
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue  
  
# grep /systemd-sulogin-shell /usr/lib/systemd/system/emergency.service  
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency
```

Remediation:

Edit `/usr/lib/systemd/system/rescue.service` and add/modify the following line:

```
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue
```

Edit `/usr/lib/systemd/system/emergency.service` and add/modify the following line:

```
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.4 Ensure the encrypted grub superusers password is set for systems booted with UEFI (Automated)

Profile Applicability:

- STIG

Description:

Operating systems booted with the Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user mode and maintenance.

Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 8 operating systems and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Audit:

For systems that use BIOS, this is Not Applicable.

Check to see if an encrypted grub superusers password is set. On systems that use UEFI, use the following command:

```
# grep -iw grub2_password /boot/efi/EFI/redhat/user.cfg  
GRUB2_PASSWORD=grub.pbkdf2.sha512.[password_hash]
```

If the grub superusers password does not begin with "grub.pbkdf2.sha512", this is a finding.

Remediation:

Configure the system to require a grub bootloader password for the grub superusers account with the grub2-setpassword command, which creates/overwrites the "/boot/efi/EFI/redhat/user.cfg" file.

Generate an encrypted grub2 password for the grub superusers account with the following command:

```
# grub2-setpassword  
Enter password:  
Confirm password:
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230234

Rule ID: SV-230234r743922_rule

STIG ID: RHEL-08-010140

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.5 Ensure the encrypted grub superusers password is set for system booted with BIOS (Automated)

Profile Applicability:

- STIG

Description:

Operating systems booted with a BIOS must require authentication upon booting into single-user and maintenance modes.

Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 8 operating systems and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Audit:

For systems that use UEFI, this is Not Applicable.

Check to see if an encrypted grub superusers password is set. On systems that use a BIOS, use the following command:

```
# grep -iw grub2_password /boot/grub2/user.cfg  
GRUB2_PASSWORD=grub.pbkdf2.sha512.[password_hash]
```

If the grub superusers password does not begin with "grub.pbkdf2.sha512", this is a finding.

Remediation:

Configure the system to require a grub bootloader password for the grub superusers account with the grub2-setpassword command, which creates/overwrites the "/boot/grub2/user.cfg" file.

Generate an encrypted grub2 password for the grub superusers account with the following command:

```
# grub2-setpassword  
Enter password:  
Confirm password:
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230235

Rule ID: SV-230235r743925_rule

STIG ID: RHEL-08-010150

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.6 Ensure the operating system requires authentication for rescue mode (Automated)

Profile Applicability:

- STIG

Description:

The operating system must require authentication upon booting into rescue mode.

Rationale:

If the system does not require valid root authentication before it boots into emergency or rescue mode, anyone who invokes emergency or rescue mode is granted privileged access to all files on the system.

Audit:

Check to see if the system requires authentication for rescue mode with the following command:

```
# grep sulogin-shell /usr/lib/systemd/system/rescue.service  
ExecStart=/usr/lib/systemd/systemd-sulogin-shell rescue
```

If the "ExecStart" line is configured for anything other than "/usr/lib/systemd/systemd-sulogin-shell rescue", commented out, or missing, this is a finding.

Remediation:

Configure the system to require authentication upon booting into rescue mode by adding the following line to the "/usr/lib/systemd/system/rescue.service" file.

```
ExecStart=/usr/lib/systemd/systemd-sulogin-shell rescue
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230236

Rule ID: SV-230236r743928_rule

STIG ID: RHEL-08-010151

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.7 Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities (Automated)

Profile Applicability:

- STIG

Description:

The operating system must clear the page allocator to prevent use-after-free attacks.

Rationale:

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Poisoning writes an arbitrary value to freed pages, so any modification or reference to that page after being freed or before being initialized will be detected and prevented. This prevents many types of use-after-free vulnerabilities at little performance cost. Also prevents leak of data and detection of corrupted memory.

Satisfies: SRG-OS-000134-GPOS-00068, SRG-OS-000433-GPOS-00192

Audit:

Verify that GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities with the following commands:

Check that the current GRUB 2 configuration has page poisoning enabled:

```
# grub2-editenv - list | grep page_poison  
  
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto  
resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb  
quiet fips=1 page_poison=1 vsyscall=none audit=1 audit_backlog_limit=8192  
boot=UUID=8d171156-cd61-421c-ba41-1c021ac29e82
```

If "page_poison" is not set to "1" or is missing, this is a finding.

Check that page poisoning is enabled by default to persist in kernel updates:

```
# grep page_poison /etc/default/grub  
  
GRUB_CMDLINE_LINUX="page_poison=1"
```

If "page_poison" is not set to "1", is missing or commented out, this is a finding.

Remediation:

Configure the operating system to enable page poisoning with the following commands:

```
# grubvy --update-kernel=ALL --args="page_poison=1"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="page_poison=1"
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230277

Rule ID: SV-230277r627750_rule

STIG ID: RHEL-08-010421

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.1 Establish and Maintain a Secure Configuration Process</p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v7	<p>5.1 Establish Secure Configurations</p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>	●	●	●

1.5.8 Ensure GRUB 2 is configured to disable vsyscalls (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable virtual syscalls.

Rationale:

Syscalls are special routines in the Linux kernel, which userspace applications ask to do privileged tasks. Invoking a system call is an expensive operation because the processor must interrupt the currently executing task and switch context to kernel mode and then back to userspace after the system call completes. Virtual syscalls map into user space a page that contains some variables and the implementation of some system calls. This allows the system calls to be executed in userspace to alleviate the context switching expense.

Virtual syscalls provide an opportunity of attack for a user who has control of the return instruction pointer. Disabling vsyscalls help to prevent return oriented programming (ROP) attacks via buffer overflows and overruns. If the system intends to run containers based on RHEL 6 components, then virtual syscalls will need to be enabled so the components function properly.

Satisfies: SRG-OS-000134-GPOS-00068, SRG-OS-000433-GPOS-00192

Audit:

Verify that GRUB 2 is configured to disable vsyscalls with the following commands:

Check that the current GRUB 2 configuration disables vsyscalls:

```
# grub2-editenv - list | grep vsyscall  
  
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto  
resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb  
quiet fips=1 page_poison=1 vsyscall=none audit=1 audit_backlog_limit=8192  
boot=UUID=8d171156-cd61-421c-ba41-1c021ac29e82
```

If "vsyscall" is not set to "none" or is missing, this is a finding.

Check that vsyscalls are disabled by default to persist in kernel updates:

```
# grep vsyscall /etc/default/grub  
  
GRUB_CMDLINE_LINUX="vsyscall=none"
```

If "vsyscall" is not set to "none", is missing or commented out and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the use of vsyscalls with the ISSO as an operational requirement or disable them with the following command:

```
# grubby --update-kernel=ALL --args="vsyscall=none"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="vsyscall=none"
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230278

Rule ID: SV-230278r743948_rule

STIG ID: RHEL-08-010422

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.9 Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities (Automated)

Profile Applicability:

- STIG

Description:

The operating system must clear SLUB/SLAB objects to prevent use-after-free attacks.

Rationale:

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Poisoning writes an arbitrary value to freed pages, so any modification or reference to that page after being freed or before being initialized will be detected and prevented. This prevents many types of use-after-free vulnerabilities at little performance cost. Also prevents leak of data and detection of corrupted memory.

SLAB objects are blocks of physically-contiguous memory. SLUB is the unqueued SLAB allocator.

Satisfies: SRG-OS-000134-GPOS-00068, SRG-OS-000433-GPOS-00192

Audit:

Verify that GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities with the following commands:

Check that the current GRUB 2 configuration has poisoning of SLUB/SLAB objects enabled:

```
# grub2-editenv - list | grep slub_debug  
  
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto  
resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb  
quiet fips=1 slub_debug=P page_poison=1 vsyscall=none audit=1  
audit_backlog_limit=8192 boot=UUID=8d171156-cd61-421c-ba41-1c021ac29e82
```

If "slub_debug" is not set to "P" or is missing, this is a finding.

Check that poisoning of SLUB/SLAB objects is enabled by default to persist in kernel updates:

```
# grep slub_debug /etc/default/grub  
  
GRUB_CMDLINE_LINUX="slub_debug=P"
```

If "slub_debug" is not set to "P", is missing or commented out, this is a finding.

Remediation:

Configure the operating system to enable poisoning of SLUB/SLAB objects with the following commands:

```
# grubby --update-kernel=ALL --args="slub_debug=P"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="slub_debug=P"
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230279

Rule ID: SV-230279r627750_rule

STIG ID: RHEL-08-010423

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.10 Ensure the operating system is configured to boot to the command line (Automated)

Profile Applicability:

- STIG

Description:

The graphical display manager must not be installed unless it is approved.

Rationale:

Internet services that are not required for system or application processes must not be active to decrease the attack surface of the system. Graphical display managers have a long history of security vulnerabilities and must not be used, unless approved and documented.

Audit:

Verify that the system is configured to boot to the command line:

```
# systemctl get-default  
multi-user.target
```

If the system default target is not set to "multi-user.target" and the Information System Security Officer (ISSO) lacks a documented requirement for a graphical user interface, this is a finding.

Verify that a graphical user interface is not installed:

```
# rpm -qa | grep xorg | grep server
```

Ask the System Administrator if use of a graphical user interface is an operational requirement.

If the use of a graphical user interface on the system is not documented with the ISSO, this is a finding.

Remediation:

Document the requirement for a graphical user interface with the ISSO or reinstall the operating system without the graphical user interface. If reinstallation is not feasible, then continue with the following procedure:

Open an SSH session and enter the following commands:

```
# systemctl set-default multi-user.target  
  
# dnf remove xorg-x11-server-Xorg xorg-x11-server-common xorg-x11-server-utils xorg-x11-server-Xwayland
```

A reboot is required for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230553

Rule ID: SV-230553r646886_rule

STIG ID: RHEL-08-040320

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.11 Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed (Automated)

Profile Applicability:

- STIG

Description:

The x86 Ctrl-Alt-Delete key sequence must be disabled.

Rationale:

A locally logged-on user, who presses Ctrl-Alt-Delete when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot.

In a graphical user environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Audit:

Verify the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed with the following command:

```
# systemctl status ctrl-alt-del.target  
  
ctrl-alt-del.target  
Loaded: masked (Reason: Unit ctrl-alt-del.target is masked.)  
Active: inactive (dead)
```

If the "ctrl-alt-del.target" is loaded and not masked, this is a finding.

Remediation:

Configure the system to disable the Ctrl-Alt-Delete sequence for the command line with the following command:

```
# systemctl mask ctrl-alt-del.target
```

Created symlink /etc/systemd/system/ctrl-alt-del.target -> /dev/null
Reload the daemon for this change to take effect.

```
# systemctl daemon-reload
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230529

Rule ID: SV-230529r627750_rule

STIG ID: RHEL-08-040170

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.12 Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds (Automated)

Profile Applicability:

- STIG

Description:

The systemd Ctrl-Alt-Delete burst key sequence must be disabled.

Rationale:

A locally logged-on user who presses Ctrl-Alt-Delete when at the console can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot.

In a graphical user environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Audit:

Verify the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds with the following command:

```
# grep -i ctrl /etc/systemd/system.conf  
CtrlAltDelBurstAction=none
```

If the "CtrlAltDelBurstAction" is not set to "none", commented out, or is missing, this is a finding.

Remediation:

Configure the system to disable the CtrlAltDelBurstAction by added or modifying the following line in the "/etc/systemd/system.conf" configuration file:

```
CtrlAltDelBurstAction=none
```

Reload the daemon for this change to take effect.

```
# systemctl daemon-reload
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230531

Rule ID: SV-230531r627750_rule

STIG ID: RHEL-08-040172

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.13 Ensure a unique name is set as the "superusers" account (UEFI) (Automated)

Profile Applicability:

- STIG

Description:

Operating systems booted with United Extensible Firmware Interface (UEFI) must require a unique superusers name upon booting into single-user mode and maintenance.

Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 8 operating systems and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Audit:

For systems that use BIOS, this is Not Applicable.

Verify that a unique name is set as the "superusers" account:

```
# grep -iw "superusers" /boot/efi/EFI/redhat/grub.cfg
set superusers="[someuniquestringhere]"
export superusers
```

If "superusers" is not set to a unique name or is missing a name, this is a finding.

Remediation:

Configure the system to have a unique name for the grub superusers account.

Edit the /etc/grub.d/01_users file and add or modify the following lines:

```
set superusers="[someuniquestringhere]"
export superusers
password_pbkdf2 [someuniquestringhere] ${GRUB2_PASSWORD}
```

Generate a new grub.cfg file with the following command:

```
# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244521

Rule ID: SV-244521r743812_rule

STIG ID: RHEL-08-010141

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.14 Ensure a unique name is set as the "superusers" account (BIOS) (Automated)

Profile Applicability:

- STIG

Description:

Operating systems booted with a BIOS must require a unique superusers name upon booting into single-user and maintenance modes.

Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 8 operating systems and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Audit:

For systems that use UEFI, this is Not Applicable.

Verify that a unique name is set as the "superusers" account:

```
# grep -iw "superusers" /boot/grub2/grub.cfg
set superusers="[someuniquestringhere]"
export superusers
```

If "superusers" is not set to a unique name or is missing a name, this is a finding.

Remediation:

Configure the system to have a unique name for the grub superusers account.

Edit the /etc/grub.d/01_users file and add or modify the following lines:

```
set superusers="[someuniquestringhere]"
export superusers
password_pbkdf2 [someuniquestringhere] ${GRUB2_PASSWORD}
```

Generate a new grub.cfg file with the following command:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244522

Rule ID: SV-244522r743815_rule

STIG ID: RHEL-08-010149

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.15 Ensure the operating system requires authentication upon booting into emergency mode (Automated)

Profile Applicability:

- STIG

Description:

The operating system must require authentication upon booting into emergency mode.

Rationale:

If the system does not require valid root authentication before it boots into emergency or rescue mode, anyone who invokes emergency or rescue mode is granted privileged access to all files on the system.

Audit:

Check to see if the system requires authentication for emergency mode with the following command:

```
# grep sulogin-shell /usr/lib/systemd/system/emergency.service  
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency
```

If the "ExecStart" line is configured for anything other than "/usr/lib/systemd/systemd-sulogin-shell emergency", commented out, or missing, this is a finding.

Remediation:

Configure the system to require authentication upon booting into emergency mode by adding the following line to the "/usr/lib/systemd/system/emergency.service" file.

```
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244523

Rule ID: SV-244523r743818_rule

STIG ID: RHEL-08-010152

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.6 Additional Process Hardening

1.6.1 Ensure core dumps are restricted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user.

Rationale:

Setting a hard limit on core dumps prevents users from overriding the soft variable. If core dumps are required, consider setting limits for user groups (see `limits.conf(5)`). In addition, setting the `fs.suid_dumpable` variable to 0 will prevent setuid programs from dumping core.

Audit:

Run the following commands and verify output matches:

```
# grep -E "^\s*\*\s+hard\s+core" /etc/security/limits.conf  
/etc/security/limits.d/*  
  
* hard core 0  
  
# sysctl fs.suid_dumpable  
  
fs.suid_dumpable = 0  
  
# grep "fs\.suid_dumpable" /etc/sysctl.conf /etc/sysctl.d/*  
  
fs.suid_dumpable = 0
```

Run the following command to check if `systemd-coredump` is installed:

```
# systemctl is-enabled coredump.service
```

if `enabled` or `disabled` is returned `systemd-coredump` is installed

Remediation:

Add the following line to `/etc/security/limits.conf` or a `/etc/security/limits.d/*` file:

```
* hard core 0
```

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
fs.suid_dumpable = 0
```

Run the following command to set the active kernel parameter:

```
# sysctl -w fs.suid_dumpable=0
```

If `systemd-coredump` is installed:

edit `/etc/systemd/coredump.conf` and add/modify the following lines:

```
Storage=none  
ProcessSizeMax=0
```

Run the command:

```
systemctl daemon-reload
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.6.2 Ensure address space layout randomization (ASLR) is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process.

Rationale:

Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

Audit:

Run the following commands and verify output matches:

```
# sysctl kernel.randomize_va_space  
kernel.randomize_va_space = 2  
  
# grep "kernel\.randomize_va_space" /etc/sysctl.conf /etc/sysctl.d/*  
kernel.randomize_va_space = 2
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
kernel.randomize_va_space = 2
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.randomize_va_space=2
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230280

Rule ID: SV-230280r627750_rule

STIG ID: RHEL-08-010430

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.6.3 Ensure the operating system disables the storing core dumps (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable the kernel.core_pattern.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Audit:

Verify the operating system disables storing core dumps with the following commands:

```
# sysctl kernel.core_pattern
kernel.core_pattern = |/bin/false
```

If the returned line does not have a value of "|/bin/false", or a line is not returned and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the operating system to disable the storing core dumps by adding the following line to a file in the "/etc/sysctl.d" directory:

```
kernel.core_pattern = |/bin/false
```

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
# sysctl --system
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230311

Rule ID: SV-230311r792894_rule

STIG ID: RHEL-08-010671

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.6.4 Ensure the operating system is not configured to acquire, save, or process core dumps (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable acquiring, saving, and processing core dumps.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

When the kernel invokes `systemd-coredump` to handle a core dump, it runs in privileged mode, and will connect to the socket created by the `systemd-coredump.socket` unit. This, in turn, will spawn an unprivileged `systemd-coredump@.service` instance to process the core dump.

Audit:

Verify the operating system is not configured to acquire, save, or process core dumps with the following command:

```
# systemctl status systemd-coredump.socket  
  
systemd-coredump.socket  
Loaded: masked (Reason: Unit ctrl-alt-del.target is masked.)  
Active: inactive (dead)
```

If "systemd-coredump.socket" is loaded and not masked and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the system to disable "systemd-coredump.socket" with the following command:

```
# systemctl mask systemd-coredump.socket  
Created symlink /etc/systemd/system/systemd-coredump.socket -> /dev/null
```

Reload the daemon for this change to take effect.

```
# systemctl daemon-reload
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230312

Rule ID: SV-230312r627750_rule

STIG ID: RHEL-08-010672

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.6.5 Ensure kernel core dumps are disabled unless needed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable kernel dumps unless needed.

Rationale:

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system partition.

The operating system's installation media presents the option to enable or disable the "kdump" service at the time of system installation.

Audit:

Verify that kernel core dumps are disabled unless needed with the following command:

```
# sudo systemctl status kdump.service

kdump.service - Crash recovery kernel arming
Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor
preset: enabled)
Active: active (exited) since Mon 2020-05-04 16:08:09 EDT; 3min ago
Main PID: 1130 (code=exited, status=0/SUCCESS)
```

If the "kdump" service is active, ask the System Administrator if the use of the service is required and documented with the Information System Security Officer (ISSO).

If the service is active and is not documented, this is a finding.

Remediation:

If kernel core dumps are not required, disable the "kdump" service with the following command:

```
# systemctl disable kdump.service
```

If kernel core dumps are required, document the need with the ISSO.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230310

Rule ID: SV-230310r627750_rule

STIG ID: RHEL-08-010670

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.6.6 Ensure the operating system disables core dumps for all users (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable core dumps for all users.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

Audit:

Verify the operating system disables core dumps for all users by issuing the following command:

```
# grep -r -s '^[^#].*core' /etc/security/limits.conf  
/etc/security/limits.d/*.conf  
  
* hard core 0
```

This can be set as a global domain (with the * wildcard) but may be set differently for multiple domains.

If the "core" item is missing, commented out, or the value is anything other than "0" and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement for all domains that have the "core" item assigned, this is a finding.

Remediation:

Configure the operating system to disable core dumps for all users.

Add the following line to the top of the "/etc/security/limits.conf" file or in a ".conf" file defined in "/etc/security/limits.d/":

```
* hard core 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230313

Rule ID: SV-230313r627750_rule

STIG ID: RHEL-08-010673

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.6.7 Ensure the operating system disables storing core dumps for all users (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable storing core dumps.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

Audit:

Verify the operating system disables storing core dumps for all users by issuing the following command:

```
# grep -i storage /etc/systemd/coredump.conf  
Storage=none
```

If the "Storage" item is missing, commented out, or the value is anything other than "none" and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement for all domains that have the "core" item assigned, this is a finding.

Remediation:

Configure the operating system to disable storing core dumps for all users.

Add or modify the following line in "/etc/systemd/coredump.conf":

```
Storage=none
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230314

Rule ID: SV-230314r627750_rule

STIG ID: RHEL-08-010674

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.6.8 Ensure the operating system disables core dump backtraces (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable core dump backtraces.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

Audit:

Verify the operating system disables core dump backtraces by issuing the following command:

```
# grep -i ProcessSizeMax /etc/systemd/coredump.conf
ProcessSizeMax=0
```

If the "ProcessSizeMax" item is missing, commented out, or the value is anything other than "0" and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement for all domains that have the "core" item assigned, this is a finding.

Remediation:

Configure the operating system to disable core dump backtraces.

Add or modify the following line in "/etc/systemd/coredump.conf":

```
ProcessSizeMax=0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230315

Rule ID: SV-230315r627750_rule

STIG ID: RHEL-08-010675

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.7 Mandatory Access Control

Mandatory Access Control (MAC) provides an additional layer of access restrictions to processes on top of the base Discretionary Access Controls. By restricting how processes can access files and resources on a system the potential impact from vulnerabilities in the processes can be reduced.

Impact: Mandatory Access Control limits the capabilities of applications and daemons on a system, while this can prevent unauthorized access the configuration of MAC can be complex and difficult to implement correctly preventing legitimate access from occurring.

1.7.1 Configure SELinux

SELinux implements Mandatory Access Control (MAC). Every process and system resource has a special security label called an SELinux context. A SELinux context, sometimes referred to as an SELinux label, is an identifier which abstracts away the system-level details and focuses on the security properties of the entity. Not only does this provide a consistent way of referencing objects in the SELinux policy, but it also removes any ambiguity that can be found in other identification methods. For example, a file can have multiple valid path names on a system that makes use of bind mounts.

The SELinux policy uses these contexts in a series of rules which define how processes can interact with each other and the various system resources. By default, the policy does not allow any interaction unless a rule explicitly grants access.

In Fedora 28 Family Linux distributions, system services are controlled by the `systemd` daemon; `systemd` starts and stops all services, and users and processes communicate with `systemd` using the `systemctl` utility. The `systemd` daemon can consult the SELinux policy and check the label of the calling process and the label of the unit file that the caller tries to manage, and then ask SELinux whether or not the caller is allowed the access. This approach strengthens access control to critical system capabilities, which include starting and stopping system services.

This automatically limits the damage that the software can do to files accessible by the calling user. The user does not need to take any action to gain this benefit. For an action to occur, both the traditional DAC permissions must be satisfied as well as the SELinux MAC rules. The action will not be allowed if either one of these models does not permit the action. In this way, SELinux rules can only make a system's permissions more restrictive and secure. SELinux requires a complex policy to allow all the actions required of a system under normal operation. Two such policies have been designed for use with Fedora 28 Family Linux distributions and are included with the system: `targeted` and `mls`. These are described as follows:

- `targeted`: targeted processes run in their own domain, called a confined domain. In a confined domain, the files that a targeted process has access to are limited. If a confined process is compromised by an attacker, the attacker's access to resources and the possible damage they can do is also limited. SELinux denies access to these resources and logs the denial.
- `mls`: implements Multi-Level Security (MLS), which introduces even more kinds of labels (sensitivity and category) and rules that govern access based on these.

This section provides guidance for the configuration of the `targeted` policy.

Notes:

- Remember that SELinux policy rules are checked after DAC rules. SELinux policy rules are not used if DAC rules deny access first, which means that no SELinux denial is logged if the traditional DAC rules prevent the access.
- This section only applies if SELinux is in use on the system. Additional Mandatory Access Control systems exist.
- To avoid incorrect SELinux labeling and subsequent problems, ensure that you start services using a systemctl start command.

References:

1. NSA SELinux resources:
 1. <http://www.nsa.gov/research/selinux>
 2. <http://www.nsa.gov/research/selinux/list.shtml>
2. Fedora SELinux resources:
 1. FAQ: <http://docs.fedoraproject.org/selinux-faq>
 2. User Guide: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html-single/using_selinux/index
 3. Managing Services Guide: <http://docs.fedoraproject.org/selinux-managing-confined-services-guide>
3. SELinux Project web page and wiki:
 1. <http://www.selinuxproject.org>

1.7.1.1 Ensure SELinux is installed (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

SELinux provides Mandatory Access Control.

Rationale:

Without a Mandatory Access Control system installed only the default Discretionary Access Control system will be available.

Audit:

Verify SELinux is installed.

Run the following command:

```
# rpm -q libselinux  
libselinux-<version>
```

Remediation:

Run the following command to install SELinux:

```
# dnf install libselinux
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

1.7.1.2 Ensure SELinux is not disabled in bootloader configuration (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Configure SELINUX to be enabled at boot time and verify that it has not been overwritten by the grub boot parameters.

Rationale:

SELinux must be enabled at boot time in your grub configuration to ensure that the controls it provides are not overridden.

Audit:

Run the following command and verify that no linux line has the `selinux=0` or `enforcing=0` parameters set:

```
# grep -E 'kernelopts=(\S+\s+)*\s*(selinux=0|enforcing=0)+\b'  
/boot/grub2/grubenv
```

Nothing should be returned

Remediation:

Edit `/etc/default/grub` and remove all instances of `selinux=0` and `enforcing=0` from all `CMDLINE_LINUX` parameters:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet"  
GRUB_CMDLINE_LINUX=""
```

Run the following command to update the `grub2` configuration:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

Additional Information:

This recommendation is designed around the grub 2 bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

1.7.1.3 Ensure SELinux policy is configured (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Configure SELinux to meet or exceed the default targeted policy, which constrains daemons and system software only.

Rationale:

Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that at least the default recommendations are met.

Audit:

Run the following commands and ensure output matches either "targeted" or "mls":

```
# grep -E '^s*SELINUXTYPE=(targeted|mls)\b' /etc/selinux/config  
SELINUXTYPE=targeted  
  
# sestatus | grep Loaded  
  
Loaded policy name:           targeted
```

Remediation:

Edit the `/etc/selinux/config` file to set the SELINUXTYPE parameter:

```
SELINUXTYPE=targeted
```

Additional Information:

If your organization requires stricter policies, ensure that they are set in the `/etc/selinux/config` file.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

1.7.1.4 Ensure the SELinux state is enforcing (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

Description:

Set SELinux to enable when the system is booted.

Rationale:

SELinux must be enabled at boot time to ensure that the controls it provides are in effect at all times.

Audit:

Run the following commands and ensure output matches:

```
# grep -E '^s*SELINUX=enforcing' /etc/selinux/config
SELINUX=enforcing

# sestatus
SELinux status: enabled
Current mode: enforcing
Mode from config file: enforcing
```

Remediation:

Edit the `/etc/selinux/config` file to set the SELINUX parameter:

```
SELINUX=enforcing
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230240

Rule ID: SV-230240r627750_rule

STIG ID: RHEL-08-010170

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists</p> <p>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>			
v7	<p>14.6 Protect Information through Access Control Lists</p> <p>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.</p>			

1.7.1.5 Ensure no unconfined services exist (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Unconfined processes run in unconfined domains

Rationale:

For unconfined processes, SELinux policy rules are applied, but policy rules exist that allow processes running in unconfined domains almost all access. Processes running in unconfined domains fall back to using DAC rules exclusively. If an unconfined process is compromised, SELinux does not prevent an attacker from gaining access to system resources and data, but of course, DAC rules are still used. SELinux is a security enhancement on top of DAC rules – it does not replace them

Audit:

Run the following command and verify no output is produced:

```
# ps -eZ | grep unconfined_service_t
```

Remediation:

Investigate any unconfined processes found during the audit action. They may need to have an existing security context assigned to them or a policy built for them.

Additional Information:

Occasionally certain daemons such as backup or centralized management software may require running unconfined. Any such software should be carefully analyzed and documented before such an exception is made.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.7.1.6 Ensure SETroubleshoot is not installed (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The SETroubleshoot service notifies desktop users of SELinux denials through a user-friendly interface. The service provides important information around configuration errors, unauthorized intrusions, and other potential errors.

Rationale:

The SETroubleshoot service is an unnecessary daemon to have running on a server, especially if X Windows is disabled.

Audit:

Verify `setroubleshoot` is not installed.

Run the following command:

```
# rpm -q setroubleshoot  
package setroubleshoot is not installed
```

Remediation:

Run the following command to uninstall `setroubleshoot`:

```
# dnf remove setroubleshoot
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>14.6 Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

1.7.1.7 Ensure the MCS Translation Service (mcstrans) is not installed (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `mcstransd` daemon provides category label information to client processes requesting information. The label translations are defined in `/etc/selinux/targeted/setrans.conf`

Rationale:

Since this service is not used very often, remove it to reduce the amount of potentially vulnerable code running on the system.

Audit:

Verify `mcstrans` is not installed.

Run the following command:

```
# rpm -q mcstrans  
package mcstrans is not installed
```

Remediation:

Run the following command to uninstall `mcstrans`:

```
# dnf remove mcstrans
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.7.1.8 Ensure the operating system has the policycoreutils package installed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must have the policycoreutils package installed.

Rationale:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

Policycoreutils contains the policy core utilities that are required for basic operation of an SELinux-enabled system. These utilities include load_policy to load SELinux policies, setfile to label filesystems, newrole to switch roles, and run_init to run "/etc/init.d" scripts in the proper context.

Audit:

Verify the operating system has the policycoreutils package installed with the following command:

```
# dnf list installed policycoreutils  
policycoreutils.x86_64 2.9-3.el8 @anaconda
```

If the policycoreutils package is not installed, this is a finding.

Remediation:

Configure the operating system to have the policycoreutils package installed with the following command:

```
# dnf install policycoreutils
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230241

Rule ID: SV-230241r627750_rule

STIG ID: RHEL-08-010171

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

1.8 Command Line Warning Banners

The /etc/motd, /etc/issue, and /etc/issue.net files govern warning banners for standard command line logins for both local and remote users.

1.8.1 Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon (Automated)

Profile Applicability:

- STIG

Description:

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon.

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Audit:

Verify the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon. Check that the operating system displays a banner at the command line login screen with the following command:

```
# cat /etc/issue
```

If the banner is set correctly it will return the following text:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

If the banner text does not match the Standard Mandatory DoD Notice and Consent Banner exactly, this is a finding.

Remediation:

Configure the operating system to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system via command line logon.

Edit the "/etc/issue" file to replace the default text with the Standard Mandatory DoD Notice and Consent Banner. The DoD-required text is:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- At any time, the USG may inspect and seize data stored on this IS.

- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

- This IS includes security measures (e.g., authentication and access controls) to protect USG interests -- not for your personal benefit or privacy.

- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230227

Rule ID: SV-230227r627750_rule

STIG ID: RHEL-08-010060

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.8.2 Ensure message of the day is configured properly (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the "`uname -a`" command once they have logged in.

Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/motd
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\\v|\\\r|\\\m|\\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's///g'))" /etc/motd
```

Remediation:

Edit the `/etc/motd` file with the appropriate contents according to your site policy, remove any instances of `\m`, `\r`, `\s`, `\v` or references to the OS platform

Or

If the motd is not used, this file can be removed.

Run the following command to remove the motd file:

```
# rm /etc/motd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.8.3 Ensure local login warning banner is configured properly (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version - or the operating system's name

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the "`uname -a`" command once they have logged in.

Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\\\v|\\\\r|\\\\m|\\\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's///g'))" /etc/issue
```

Remediation:

Edit the `/etc/issue` file with the appropriate contents according to your site policy, remove any instances of `\m`, `\r`, `\s`, `\v` or references to the OS platform

```
# echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.8.4 Ensure remote login warning banner is configured properly (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the "`uname -a`" command once they have logged in.

Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue.net
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\\\v|\\\\r|\\\\m|\\\\s|$|grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's///g'))" /etc/issue.net
```

Remediation:

Edit the `/etc/issue.net` file with the appropriate contents according to your site policy, remove any instances of `\m`, `\r`, `\s`, `\v` or references to the OS platform

```
# echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue.net
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.1 Establish and Maintain a Secure Configuration Process</p> <p>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v7	<p>5.1 Establish Secure Configurations</p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>	●	●	●

1.8.5 Ensure permissions on /etc/motd are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

Rationale:

If the `/etc/motd` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access is 644`:

```
# stat /etc/motd
Access: (0644/-rw-r--r--)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/motd`:

```
# chown root:root /etc/motd
# chmod u-x,go-wx /etc/motd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.8.6 Ensure permissions on /etc/issue are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

Rationale:

If the `/etc/issue` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644`:

```
# stat /etc/issue
Access: (0644/-rw-r--r--)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/issue`:

```
# chown root:root /etc/issue
# chmod u-rw,go-wx /etc/issue
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.8.7 Ensure permissions on /etc/issue.net are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

Rationale:

If the `/etc/issue.net` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access is 644`:

```
# stat /etc/issue.net
Access: (0644/-rw-r--r--)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/issue.net`:

```
# chown root:root /etc/issue.net
# chmod u-x,go-wx /etc/issue.net
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.8.8 Ensure the Standard Mandatory DoD Notice and Consent Banner is displayed before granting access to the system via SSH logon (Automated)

Profile Applicability:

- STIG

Description:

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a ssh logon.

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agree'm't."

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Audit:

Verify any publicly accessible connection to the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the system.
Check for the location of the banner file being used with the following command:

```
# grep -i banner /etc/ssh/sshd_config  
banner /etc/issue
```

This command will return the banner keyword and the name of the file that contains the ssh banner (in this case "/etc/issue").

If the line is commented out, this is a finding.

View the file specified by the banner keyword to check that it matches the text of the Standard Mandatory DoD Notice and Consent Banner:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.  
  
-At any time, the USG may inspect and seize data stored on this IS.  
  
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.  
  
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.  
  
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."
```

If the system does not display a graphical logon banner or the banner does not match the Standard Mandatory DoD Notice and Consent Banner, this is a finding.

If the text in the file does not match the Standard Mandatory DoD Notice and Consent Banner, this is a finding.

Remediation:

Configure the operating system to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system via the ssh.

Edit the "/etc/ssh/sshd_config" file to uncomment the banner keyword and configure it to point to a file that will contain the logon banner (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor). An example configuration line is:

```
banner /etc/issue
```

Either create the file containing the banner or replace the text in the file with the Standard Mandatory DoD Notice and Consent Banner. The DoD-required text is:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

The SSH service must be restarted for changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230225

Rule ID: SV-230225r627750_rule

STIG ID: RHEL-08-010040

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.8.9 Ensure the operating system displays a banner before granting access to the operating system via a graphical user logon (Automated)

Profile Applicability:

- STIG

Description:

The operating system must display a banner before granting local or remote access to the system via a graphical user logon.

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Audit:

Verify the operating system displays a banner before granting access to the operating system via a graphical user logon.

Note: This requirement assumes the use of the operating system's default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Check to see if the operating system displays a banner at the logon screen with the following command:

```
# grep banner-message-enable /etc/dconf/db/local.d/*
banner-message-enable=true
```

If "banner-message-enable" is set to "false" or is missing, this is a finding.

Remediation:

Configure the operating system to display a banner before granting access to the system.

Note: If the system does not have a graphical user interface installed, this requirement is Not Applicable.

Create a database to contain the system-wide graphical user logon settings (if it does not already exist) with the following command:

```
# touch /etc/dconf/db/local.d/01-banner-message
```

Add the following lines to the [org/gnome/login-screen] section of the "/etc/dconf/db/local.d/01-banner-message":

```
[org/gnome/login-screen]
banner-message-enable=true
```

Run the following command to update the database:

```
# dconf update
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244519

Rule ID: SV-244519r743806_rule

STIG ID: RHEL-08-010049

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.9 GNOME Display Manager

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

The system will need to be re-booted, or brought down to run level 3 and back to run level 5 for changes to the GDM configuration to take effect.

Note: If GDM is not installed on the system, this section can be skipped

1.9.1 Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon (Automated)

Profile Applicability:

- STIG

Description:

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Audit:

Verify the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon.

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Check that the operating system displays the exact Standard Mandatory DoD Notice and Consent Banner text with the command:

```
# sudo grep banner-message-text /etc/dconf/db/local.d/*  
  
banner-message-text=  
'You are accessing a U.S. Government (USG) Information System (IS) that is  
provided for USG-authorized use only.\nBy using this IS (which includes any  
device attached to this IS), you consent to the following conditions:\n-The  
USG routinely intercepts and monitors communications on this IS for purposes  
including, but not limited to, penetration testing, COMSEC monitoring,  
network operations and defense, personnel misconduct (PM), law enforcement  
(LE), and counterintelligence (CI) investigations.\n-At any time, the USG may  
inspect and seize data stored on this IS.\n-Communications using, or data  
stored on, this IS are not private, are subject to routine monitoring,  
interception, and search, and may be disclosed or used for any USG-authorized  
purpose.\n-This IS includes security measures (e.g., authentication and  
access controls) to protect USG interests--not for your personal benefit or  
privacy.\n-Notwithstanding the above, using this IS does not constitute  
consent to PM, LE or CI investigative searching or monitoring of the content  
of privileged communications, or work product, related to personal  
representation or services by attorneys, psychotherapists, or clergy, and  
their assistants. Such communications and work product are private and  
confidential. See User Agreement for details. '
```

Note: The "\n " characters are for formatting only. They will not be displayed on the graphical interface.

If the banner does not match the Standard Mandatory DoD Notice and Consent Banner exactly, this is a finding.

Remediation:

Configure the operating system to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system.

Note: If the system does not have a graphical user interface installed, this requirement is Not Applicable.

Add the following lines to the [org/gnome/login-screen] section of the "/etc/dconf/db/local.d/01-banner-message":

```
banner-message-text='You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.\nBy using this IS (which includes any device attached to this IS), you consent to the following conditions:\n-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.\n-At any time, the USG may inspect and seize data stored on this IS.\n-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.\n-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.\n-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. '
```

Note: The "\n" characters are for formatting only. They will not be displayed on the graphical interface.

Run the following command to update the database:

```
# dconf update
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230226

Rule ID: SV-230226r743916_rule

STIG ID: RHEL-08-010050

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.9.2 Ensure GNOME Display Manager is removed (Manual)

Profile Applicability:

- Level 2 - Server

Description:

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

Rationale:

If a Graphical User Interface (GUI) is not required, it should be removed to reduce the attack surface of the system.

Impact:

Removing the GNOME Display manager will remove the GUI from the system.

Audit:

Run the following command and verify the output:

```
# rpm -q gdm  
package gdm is not installed
```

Remediation:

Run the following command to remove the `gdm` package

```
# dnf remove gdm
```

References:

1. <https://wiki.gnome.org/Projects/GDM>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

1.9.3 Ensure GDM login banner is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place.

Note: If a graphical login is not required, it should be removed to reduce the attack surface of the system.

Audit:

Verify that a file exists in /etc/dconf/db/local.d/: (*This is typically /etc/dconf/db/local.d/01-banner-message*)

Run the following command:

```
find /etc/dconf/db/local.d/ -type f -exec grep 'banner-message-' {} \;
```

Ensure the output includes:

```
banner-message-enable=true  
banner-message-text='<banner message>'
```

Remediation:

Edit or create the file `/etc/dconf/profile/local` and add the following:

```
user-db:user
system-db:local
file-db:/usr/share/local/greeter-dconf-defaults
```

Edit or create the file `/etc/dconf/db/local.d/` and add the following: (*This is typically /etc/dconf/db/local.d/01-banner-message*)

```
[org/gnome/login-screen]
banner-message-enable=true
banner-message-text='<banner message>'
```

Example Banner Text: 'Authorized users only. All activity may be monitored and reported.'

Run the following command to update the system databases:

```
# dconf update
```

Additional Information:

Additional options and sections may appear in the `/etc/dconf/db/local.d/01-banner-message` file.

If a different GUI login service is in use and required on the system, consult your documentation to disable displaying the last logged on user and apply an equivalent banner.

Red Hat Enterprise Linux 7 Security Technical Implementation Guide

Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204393

Rule ID: SV-204393r603261_rule

STIG ID: RHEL-07-010030

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.9.4 Ensure last logged in user display is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

Rationale:

Displaying the last logged in user eliminates half of the Userid/Password equation that an unauthorized person would need to log on.

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place.

Notes:

- *If a graphical login is not required, it should be removed to reduce the attack surface of the system.*
- *If a different GUI login service is in use and required on the system, consult your documentation to disable displaying the last logged on user*

Audit:

Verify that /etc/dconf/profile/gdm exists and includes the following:

```
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

Verify that a file exists in /etc/dconf/db/gdm.d/ and includes the following: (*This is typically /etc/dconf/db/gdm.d/00-login-screen*)

```
[org/gnome/login-screen]
disable-user-list=true
```

Remediation:

Edit or create the file `/etc/dconf/profile/gdm` and add the following:

```
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

Edit or create the file `/etc/dconf/db/gdm.d/` and add the following: (*This is typically /etc/dconf/db/gdm.d/00-login-screen*)

```
[org/gnome/login-screen]
# Do not show the user list
disable-user-list=true
```

Run the following command to update the system databases:

```
# dconf update
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.9.5 Ensure XDCMP is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

X Display Manager Control Protocol (XDMCP) is designed to provide authenticated access to display management services for remote displays

Rationale:

XDMCP is inherently insecure.

- XDMCP is not a ciphered protocol. This may allow an attacker to capture keystrokes entered by a user
- XDMCP is vulnerable to man-in-the-middle attacks. This may allow an attacker to steal the credentials of legitimate users by impersonating the XDMCP server.

Audit:

Run the following command and verify the output:

```
# grep -Eis '^s*Enable\s*=\s*true' /etc/gdm/custom.conf  
Nothing should be returned
```

Remediation:

Edit the file `/etc/gdm/custom.conf` and remove the line

```
Enable=true
```

Default Value:

false (This is denoted by no `Enabled=` entry in the file `/etc/gdm/custom.conf` in the `[xdmcp]` section)

References:

1. <https://help.gnome.org/admin/gdm/2.32/configuration.html.en>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

1.9.6 Ensure a Standard Mandatory DoD Notice and Consent Banner is displayed via a graphical user logon (Manual)

Profile Applicability:

- STIG

Description:

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local access to the system via a graphical user logon.

Rationale:

Display of a standardized and approved use notification before granting access to the Ubuntu operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist. The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Audit:

Verify the Ubuntu operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon.

Note: If the system does not have a graphical user interface installed, this requirement is Not Applicable.

Verify the operating system displays the exact approved Standard Mandatory DoD Notice and Consent Banner text with the command:

```
# grep ^banner-message-text /etc/gdm3/greeter.dconf-defaults
```

Output should read:

```
banner-message-text="You are accessing a U.S. Government \ (USG\)\ Information System \ (IS\)\ that is provided for USG-authorized use only.\s+By using this IS \ (which includes any device attached to this IS\), you consent to the following conditions:\s+-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct \ (PM\), law enforcement \ (LE\), and counterintelligence \ (CI\)\ investigations.\s+-At any time, the USG may inspect and seize data stored on this IS.\s+-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.\s+-This IS includes security measures \ (e.g., authentication and access controls\)\ to protect USG interests--not for your personal benefit or privacy.\s+-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."
```

If the banner-message-text is missing, commented out, or does not match the Standard Mandatory DoD Notice and Consent Banner exactly, this is a finding.

Remediation:

Edit the "/etc/gdm3/greeter.dconf-defaults" file.

Set the "banner-message-text" line to contain the appropriate banner message text as shown below:

```
banner-message-text='You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.\n\nBy using this IS (which includes any device attached to this IS), you consent to the following conditions:\n\n-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.\n\n-At any time, the USG may inspect and seize data stored on this IS.\n\n-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.\n\n-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.\n\n-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.'
```

Update the GDM with the new configuration:

```
# dconf update
# systemctl restart gdm3
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide

Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238198

Rule ID: SV-238198r653769_rule

STIG ID: UBTU-20-010003

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.9.7 Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface (Automated)

Profile Applicability:

- STIG

Description:

Unattended or automatic logon via the operating system's graphical user interface must not be allowed.

Rationale:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Audit:

Verify the operating system does not allow an unattended or automatic logon to the system via a graphical user interface.

Note: This requirement assumes the use of the RHEL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Check for the value of the "AutomaticLoginEnable" in the "/etc/gdm/custom.conf" file with the following command:

```
# grep -i automaticloginenable /etc/gdm/custom.conf  
AutomaticLoginEnable=false
```

If the value of "AutomaticLoginEnable" is not set to "false", this is a finding.

Remediation:

Configure the operating system to not allow an unattended or automatic logon to the system via a graphical user interface.

Add or edit the line for the "AutomaticLoginEnable" parameter in the [daemon] section of the "/etc/gdm/custom.conf" file to "false":

```
[daemon]  
AutomaticLoginEnable=false
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230329

Rule ID: SV-230329r627750_rule

STIG ID: RHEL-08-010820

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.9.8 Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface (Automated)

Profile Applicability:

- STIG

Description:

The x86 Ctrl-Alt-Delete key sequence must be disabled if a graphical user interface is installed.

Rationale:

A locally logged-on user, who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In a graphical user environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Audit:

Verify the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface with the following command:

This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
# grep logout /etc/dconf/db/local.d/*
logout=''
```

If the "logout" key is bound to an action, is commented out, or is missing, this is a finding.

Remediation:

Configure the system to disable the Ctrl-Alt-Delete sequence when using a graphical user interface by creating or editing the /etc/dconf/db/local.d/00-disable-CAD file.

Add the setting to disable the Ctrl-Alt-Delete sequence for a graphical user interface:

```
[org/gnome/settings-daemon/plugins/media-keys]
logout=''
```

Note: The value above is set to two single quotations.

Then update the dconf settings:

```
# dconf update
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230530

Rule ID: SV-230530r646883_rule

STIG ID: RHEL-08-040171

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.9.9 Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated (Automated)

Profile Applicability:

- STIG

Description:

The operating system must initiate a session lock for graphical user interfaces when the screensaver is activated.

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012, SRG-OS-000480-GPOS-00227

Audit:

Verify the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated with the following command:

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
# gsettings get org.gnome.desktop.screensaver lock-delay  
uint32 5
```

If the "uint32" setting is missing, or is not set to "5" or less, this is a finding.

Remediation:

Configure the operating system to initiate a session lock for graphical user interfaces when a screensaver is activated.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/00-screensaver  
[org/gnome/desktop/screensaver]  
lock-delay=uint32 5
```

The "uint32" must be included along with the integer key values as shown.

Update the system databases:

```
# dconf update
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244535

Rule ID: SV-244535r743854_rule

STIG ID: RHEL-08-020031

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	<u>16.11 Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

1.9.10 Ensure the operating system disables the user logon list for graphical user interfaces (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable the user list at logon for graphical user interfaces.

Rationale:

Leaving the user list enabled is a security risk since it allows anyone with physical access to the system to enumerate known user accounts without authenticated access to the system.

Audit:

Verify the operating system disables the user logon list for graphical user interfaces with the following command:

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
# gsettings get org.gnome.login-screen disable-user-list  
true
```

If the setting is "false", this is a finding.

Remediation:

Configure the operating system to disable the user list at logon for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/02-login-screen  
[org/gnome/login-screen]  
disable-user-list=true
```

Update the system databases:

```
# dconf update
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244536

Rule ID: SV-244536r743857_rule

STIG ID: RHEL-08-020032

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.9.11 Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent a user from overriding the session idle-delay setting for the graphical user interface.

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Implementing session settings will have little value if a user is able to manipulate these settings from the defaults prescribed in the other requirements of this implementation guide.

Locking these settings from non-privileged users is crucial to maintaining a protected baseline.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012, SRG-OS-000480-GPOS-00227

Audit:

Verify the operating system prevents a user from overriding settings for graphical user interfaces.

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user  
system-db:local
```

Check that graphical settings are locked from non-privileged user modification with the following command:

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
# grep -i idle /etc/dconf/db/local.d/locks/*  
/org/gnome/desktop/session/idle-delay
```

If the command does not return at least the example result, this is a finding.

Remediation:

Configure the operating system to prevent a user from overriding settings for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the following setting to prevent non-privileged users from modifying it:

```
/org/gnome/desktop/session/idle-delay
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244538

Rule ID: SV-244538r743863_rule

STIG ID: RHEL-08-020081

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	<u>16.11 Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

1.9.12 Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent a user from overriding the screensaver lock-enabled setting for the graphical user interface.

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Implementing session settings will have little value if a user is able to manipulate these settings from the defaults prescribed in the other requirements of this implementation guide.

Locking these settings from non-privileged users is crucial to maintaining a protected baseline.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012, SRG-OS-000480-GPOS-00227

Audit:

Verify the operating system prevents a user from overriding settings for graphical user interfaces.

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user  
system-db:local
```

Check that graphical settings are locked from non-privileged user modification with the following command:

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
# grep -i lock-enabled /etc/dconf/db/local.d/locks/*  
/org/gnome/desktop/screensaver/lock-enabled
```

If the command does not return at least the example result, this is a finding.

Remediation:

Configure the operating system to prevent a user from overriding settings for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the following setting to prevent non-privileged users from modifying it:

```
/org/gnome/desktop/screensaver/lock-enabled
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244539

Rule ID: SV-244539r743866_rule

STIG ID: RHEL-08-020082

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	<u>16.11 Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

1.10 Ensure updates, patches, and additional security software are installed (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

Periodically patches are released for included software either due to security flaws or to include additional functionality.

Rationale:

Newer patches may contain security enhancements that would not be available through the latest full update. As a result, it is recommended that the latest software patches be used to take advantage of the latest functionality. As with any software installation, organizations need to determine if a given update meets their requirements and verify the compatibility and supportability of any additional software against the update revision that is selected.

Audit:

Run the following command and verify there are no updates or patches to install:

```
# dnf check-update
```

Remediation:

Use your package manager to update all packages on the system according to site policy. The following command will install all available updates:

```
# dnf update
```

Additional Information:

Site policy may mandate a testing period before install onto production systems for available updates.

```
# dnf check-update
```

Red Hat Enterprise Linux 8 Security Technical Implementation Guide
Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230222
Rule ID: SV-230222r627750_rule
STIG ID: RHEL-08-010010
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

1.11 Ensure system-wide crypto policy is not legacy (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The system-wide crypto-policies followed by the crypto core components allow consistently deprecating and disabling algorithms system-wide.

The individual policy levels (DEFAULT, LEGACY, FUTURE, and FIPS) are included in the crypto-policies(7) package.

Rationale:

If the Legacy system-wide crypto policy is selected, it includes support for TLS 1.0, TLS 1.1, and SSH2 protocols or later. The algorithms DSA, 3DES, and RC4 are allowed, while RSA and Diffie-Hellman parameters are accepted if larger than 1023-bits.

These legacy protocols and algorithms can make the system vulnerable to attacks, including those listed in RFC 7457

Impact:

Environments that require compatibility with older insecure protocols may require the use of the less secure LEGACY policy level.

Audit:

Run the following command to verify that the system-wide crypto policy is not LEGACY

```
# grep -E -i '^s*LEGACY\s*(\s+\#.*)?$' /etc/crypto-policies/config
```

Verify that no lines are returned

Remediation:

Run the following command to change the system-wide crypto policy

```
# update-crypto-policies --set <CRYPTO POLICY>
```

Example:

```
# update-crypto-policies --set DEFAULT
```

Run the following to make the updated system-wide crypto policy active

```
# update-crypto-policies
```

Default Value:

DEFAULT

References:

1. CRYPTO-POLICIES(7)
2. <https://access.redhat.com/articles/3642912#what-polices-are-provided-1>

Additional Information:

To switch the system to FIPS mode, run the following command:

```
fips-mode-setup --enable
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

1.12 Ensure system-wide crypto policy is FUTURE or FIPS (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The system-wide crypto-policies followed by the crypto core components allow consistently deprecating and disabling algorithms system-wide.

The individual policy levels (DEFAULT, LEGACY, FUTURE, and FIPS) are included in the crypto-policies(7) package.

Rationale:

If the Legacy system-wide crypto policy is selected, it includes support for TLS 1.0, TLS 1.1, and SSH2 protocols or later. The algorithms DSA, 3DES, and RC4 are allowed, while RSA and Diffie-Hellman parameters are accepted if larger than 1023-bits.

These legacy protocols and algorithms can make the system vulnerable to attacks, including those listed in RFC 7457

FUTURE: Is a conservative security level that is believed to withstand any near-term future attacks. This level does not allow the use of SHA-1 in signature algorithms. The RSA and Diffie-Hellman parameters are accepted if larger than 3071 bits. The level provides at least 128-bit security

FIPS: Conforms to the FIPS 140-2 requirements. This policy is used internally by the fips-mode-setup(8) tool which can switch the system into the FIPS 140-2 compliance mode. The level provides at least 112-bit security

Impact:

Environments that require compatibility with older insecure protocols may require the use of the less secure LEGACY policy level.

Systems configured to use system-wide crypto policy of Future or FIPS will no longer accept connections from openSSH clients that do not support sha2 pub key types
openSSH clients may need to explicitly override and modify PubKeyAcceptedKeyTypes to accept sha2 hashed pub keys

Audit:

Run the following command to verify that the system-wide crypto policy is Future or FIPS

```
# grep -E -i '^s*(FUTURE|FIPS)s*(\s+\#.*)?$' /etc/crypto-policies/config
```

Verify that either `FUTURE` or `FIPS` is returned

Remediation:

Run the following command to change the system-wide crypto policy

```
# update-crypto-policies --set FUTURE
```

Or

To switch the system to FIPS mode, run the following command:

```
# fips-mode-setup --enable
```

Default Value:

DEFAULT

References:

1. CRYPTO-POLICIES(7)
2. <https://access.redhat.com/articles/3642912#what-polices-are-provided-1>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

1.13 Ensure the operating system implements DoD-approved encryption (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the Federal Government since this provides assurance they have been tested and validated.

RHEL 8 utilizes GRUB 2 as the default bootloader. Note that GRUB 2 command-line parameters are defined in the "kernelopts" variable of the /boot/grub2/grubenv file for all kernel boot entries. The command "fips-mode-setup" modifies the "kernelopts" variable, which in turn updates all kernel boot entries.

The fips=1 kernel option needs to be added to the kernel command line during system installation so that key generation is done with FIPS-approved algorithms and continuous monitoring tests in place. Users must also ensure the system has plenty of entropy during the installation process by moving the mouse around, or if no mouse is available, ensuring that many keystrokes are typed. The recommended amount of keystrokes is 256 and more. Less than 256 keystrokes may generate a non-unique key.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000125-GPOS-00065, SRG-OS-000396-GPOS-00176, SRG-OS-000423-GPOS-00187, SRG-OS-000478-GPOS-00223

Audit:

Verify the operating system implements DoD-approved encryption to protect the confidentiality of remote access sessions.

Check to see if FIPS mode is enabled with the following command:

```
# fipscheck
```

```
usage: fipscheck [-s ]
```

```
fips mode is on
```

If FIPS mode is "on", check to see if the kernel boot parameter is configured for FIPS mode with the following command:

```
# grub2-editenv - list | grep fips
```

```
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto  
resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet  
fips=1 boot=UUID=8d171156-cd61-421c-ba41-1c021ac29e82
```

If the kernel boot parameter is configured to use FIPS mode, check to see if the system is in FIPS mode with the following command:

```
# cat /proc/sys/crypto/fips_enabled
```

```
1
```

If FIPS mode is not "on", the kernel boot parameter is not configured for FIPS mode, or the system does not have a value of "1" for "fips_enabled" in "/proc/sys/crypto", this is a finding.

Remediation:

Configure the operating system to implement DoD-approved encryption by following the steps below:

To enable strict FIPS compliance, the fips=1 kernel option needs to be added to the kernel boot parameters during system installation so key generation is done with FIPS-approved algorithms and continuous monitoring tests in place.

Enable FIPS mode after installation (not strict FIPS compliant) with the following command:

```
# fips-mode-setup --enable
```

Reboot the system for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230223

Rule ID: SV-230223r627750_rule

STIG ID: RHEL-08-010020

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

1.14 Ensure the operating system prevents unauthorized modification of all information at rest by using disk encryption (Manual)

Profile Applicability:

- STIG

Description:

All local disk partitions must implement cryptographic mechanisms to prevent unauthorized disclosure or modification of all information that requires at rest protection.

Rationale:

RHEL 8 systems handling data requiring "data at rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Satisfies: SRG-OS-000185-GPOS-00079, SRG-OS-000404-GPOS-00183, SRG-OS-000405-GPOS-00184

Audit:

Verify the operating system prevents unauthorized disclosure or modification of all information requiring at-rest protection by using disk encryption.

If there is a documented and approved reason for not having data-at-rest encryption, this requirement is Not Applicable.

Verify all system partitions are encrypted with the following command:

```
# blkid  
  
/dev/mapper/rhel-root: UUID="67b7d7fe-de60-6fd0-befb-e6748cf97743"  
TYPE="crypto_LUKS"
```

Every persistent disk partition present must be of type "crypto_LUKS". If any partitions other than pseudo file systems (such as /proc or /sys) are not type "crypto_LUKS", ask the administrator to indicate how the partitions are encrypted. If there is no evidence that all local disk partitions are encrypted, this is a finding.

Remediation:

Configure the operating system to prevent unauthorized modification of all information at rest by using disk encryption.

Encrypting a partition in an already installed system is more difficult, because existing partitions will need to be resized and changed. To encrypt an entire partition, dedicate a partition for encryption in the partition layout.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230224

Rule ID: SV-230224r627750_rule

STIG ID: RHEL-08-010030

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

1.15 Ensure kernel image loading is disabled (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent the loading of a new kernel for later execution.

Rationale:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Disabling kexec_load prevents an unsigned kernel image (that could be a windows kernel or modified vulnerable kernel) from being loaded. Kexec can be used subvert the entire secureboot process and should be avoided at all costs especially since it can load unsigned kernel images.

Audit:

Verify the operating system is configured to disable kernel image loading with the following commands:

Check the status of the kernel.kexec_load_disabled kernel parameter

```
# sysctl kernel.kexec_load_disabled  
kernel.kexec_load_disabled = 1
```

If "kernel.kexec_load_disabled" is not set to "1" or is missing, this is a finding.

Check that the configuration files are present to enable this kernel parameter

```
# grep -r kernel.kexec_load_disabled /etc/sysctl.conf /etc/sysctl.d/*.conf  
/etc/sysctl.d/99-sysctl.conf:kernel.kexec_load_disabled = 1
```

If "kernel.kexec_load_disabled" is not set to "1", is missing or commented out, this is a finding.

Remediation:

Configure the operating system to disable kernel image loading.

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
kernel.kexec_load_disabled = 1
```

Load settings from all system configuration files with the following command:

```
# sysctl --system
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230266

Rule ID: SV-230266r627750_rule

STIG ID: RHEL-08-010372

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.16 Ensure the operating system is configured to enable DAC on symlinks (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enable kernel parameters to enforce discretionary access control on symlinks.

Rationale:

Discretionary Access Control (DAC) is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. A subject that is constrained in its operation by Mandatory Access Control policies is still able to operate under the less rigorous constraints of this requirement. Thus, while Mandatory Access Control imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.

By enabling the `fs.protected_symlinks` kernel parameter, symbolic links are permitted to be followed only when outside a sticky world-writable directory, or when the UID of the link and follower match, or when the directory owner matches the symlink's owner.

Disallowing such symlinks helps mitigate vulnerabilities based on insecure file system accessed by privileged programs, avoiding an exploitation vector exploiting unsafe use of `open()` or `creat()`.

Satisfies: SRG-OS-000312-GPOS-00122, SRG-OS-000312-GPOS-00123, SRG-OS-000312-GPOS-00124, SRG-OS-000324-GPOS-00125

Audit:

Verify the operating system is configured to enable DAC on symlinks with the following commands:

Check the status of the `fs.protected_symlinks` kernel parameter.

```
# sysctl fs.protected_symlinks  
fs.protected_symlinks = 1
```

If "fs.protected_symlinks" is not set to "1" or is missing, this is a finding.

Check that the configuration files are present to enable this kernel parameter.

```
# grep -r fs.protected_symlinks /etc/sysctl.conf /etc/sysctl.d/*.conf  
/etc/sysctl.d/99-sysctl.conf:fs.protected_symlinks = 1
```

If "fs.protected_symlinks" is not set to "1", is missing or commented out, this is a finding.

Remediation:

Configure the operating system to enable DAC on symlinks.

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
fs.protected_symlinks = 1
```

Load settings from all system configuration files with the following command:

```
# sysctl --system
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230267

Rule ID: SV-230267r627750_rule

STIG ID: RHEL-08-010373

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

1.17 Ensure the operating system is configured to enable DAC on hardlinks (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enable kernel parameters to enforce discretionary access control on hardlinks.

Rationale:

Discretionary Access Control (DAC) is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. A subject that is constrained in its operation by Mandatory Access Control policies is still able to operate under the less rigorous constraints of this requirement. Thus, while Mandatory Access Control imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.

By enabling the `fs.protected_hardlinks` kernel parameter, users can no longer create soft or hard links to files they do not own. Disallowing such hardlinks mitigate vulnerabilities based on insecure file system accessed by privileged programs, avoiding an exploitation vector exploiting unsafe use of `open()` or `creat()`.

Satisfies: SRG-OS-000312-GPOS-00122, SRG-OS-000312-GPOS-00123, SRG-OS-000312-GPOS-00124, SRG-OS-000324-GPOS-00125

Audit:

Verify the operating system is configured to enable DAC on hardlinks with the following commands:

Check the status of the `fs.protected_hardlinks` kernel parameter.

```
# sysctl fs.protected_hardlinks  
fs.protected_hardlinks = 1
```

If "fs.protected_hardlinks" is not set to "1" or is missing, this is a finding.

Check that the configuration files are present to enable this kernel parameter.

```
# grep -r fs.protected_hardlinks /etc/sysctl.conf /etc/sysctl.d/*.conf  
/etc/sysctl.d/99-sysctl.conf:fs.protected_hardlinks = 1
```

If "fs.protected_hardlinks" is not set to "1", is missing or commented out, this is a finding.

Remediation:

Configure the operating system to enable DAC on hardlinks.

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
fs.protected_hardlinks = 1
```

Load settings from all system configuration files with the following command:

```
# sysctl --system
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230268

Rule ID: SV-230268r627750_rule

STIG ID: RHEL-08-010374

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

1.18 Ensure the operating system is configured to restrict access to the kernel message buffer (Automated)

Profile Applicability:

- STIG

Description:

The operating system must restrict access to the kernel message buffer.

Rationale:

Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Restricting access to the kernel message buffer limits access to only root. This prevents attackers from gaining additional system information as a non-privileged user.

Audit:

Verify the operating system is configured to restrict access to the kernel message buffer with the following commands:

Check the status of the kernel.dmesg_restrict kernel parameter.

```
# sysctl kernel.dmesg_restrict  
kernel.dmesg_restrict = 1
```

If "kernel.dmesg_restrict" is not set to "1" or is missing, this is a finding.

Check that the configuration files are present to enable this kernel parameter.

```
# grep -r kernel.dmesg_restrict /etc/sysctl.conf /etc/sysctl.d/*.conf  
/etc/sysctl.d/99-sysctl.conf:kernel.dmesg_restrict = 1
```

If "kernel.dmesg_restrict" is not set to "1", is missing or commented out, this is a finding.

Remediation:

Configure the operating system to restrict access to the kernel message buffer.

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
kernel.dmesg_restrict = 1
```

Load settings from all system configuration files with the following command:

```
# sysctl --system
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230269

Rule ID: SV-230269r627750_rule

STIG ID: RHEL-08-010375

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

1.19 Ensure the operating system is configured to prevent kernel profiling by unprivileged users (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent kernel profiling by unprivileged users.

Rationale:

Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Setting the kernel.perf_event_paranoia kernel parameter to "2" prevents attackers from gaining additional system information as a non-privileged user.

Audit:

Verify the operating system is configured to prevent kernel profiling by unprivileged users with the following commands:

Check the status of the kernel.perf_event_paranoid kernel parameter.

```
# sysctl kernel.perf_event_paranoid  
kernel.perf_event_paranoid = 2
```

If "kernel.perf_event_paranoid" is not set to "2" or is missing, this is a finding.

Check that the configuration files are present to enable this kernel parameter.

```
# grep -r kernel.perf_event_paranoid /etc/sysctl.conf /etc/sysctl.d/*.conf  
/etc/sysctl.d/99-sysctl.conf:kernel.perf_event_paranoid = 2
```

If "kernel.perf_event_paranoid" is not set to "2", is missing or commented out, this is a finding.

Remediation:

Configure the operating system to prevent kernel profiling by unprivileged users.

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
kernel.perf_event_paranoid = 2
```

Load settings from all system configuration files with the following command:

```
# sysctl -system
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230270

Rule ID: SV-230270r627750_rule

STIG ID: RHEL-08-010376

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

1.20 Ensure the operating system has the packages required for multifactor authentication (Automated)

Profile Applicability:

- STIG

Description:

The operating system must have the packages required for multifactor authentication installed.

Rationale:

Using an authentication device, such as a DoD Common Access Card (CAC) or token that is separate from the information system, ensures that even if the information system is compromised, credentials stored on the authentication device will not be affected.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification (PIV) card and the DoD CAC.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless. This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Audit:

Verify the operating system has the packages required for multifactor authentication installed with the following commands:

```
# dnf list installed openssl-pkcs11  
openssl-pkcs11.x86_64 0.4.8-2.el8 @anaconda
```

If the "openssl-pkcs11" package is not installed, ask the administrator to indicate what type of multifactor authentication is being utilized and what packages are installed to support it. If there is no evidence of multifactor authentication being used, this is a finding.

Remediation:

Configure the operating system to implement multifactor authentication by installing the required package with the following command:

```
# dnf install openssl-pkcs11
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230273

Rule ID: SV-230273r743943_rule

STIG ID: RHEL-08-010390

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.21 Ensure the operating system implements certificate status checking for multifactor authentication (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement certificate status checking for multifactor authentication.

Rationale:

Using an authentication device, such as a DoD Common Access Card (CAC) or token that is separate from the information system, ensures that even if the information system is compromised, credentials stored on the authentication device will not be affected.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification (PIV) card and the DoD CAC.

RHEL 8 operating systems include multiple options for configuring certificate status checking, but for this requirement focuses on the System Security Services Daemon (SSSD). By default, sssd performs Online Certificate Status Protocol (OCSP) checking and certificate verification using a sha256 digest function.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000377-GPOS-00162

Audit:

Verify the operating system implements certificate status checking for multifactor authentication.

Check to see if Online Certificate Status Protocol (OCSP) is enabled and using the proper digest value on the system with the following command:

```
# grep certificate_verification /etc/sssd/sssd.conf /etc/sssd/conf.d/*.conf |  
grep -v "^\#"  
  
certificate_verification = ocsp_dgst=sha1
```

If the certificate_verification line is missing from the [sssd] section, or is missing "ocsp_dgst=sha1", ask the administrator to indicate what type of multifactor authentication is being utilized and how the system implements certificate status checking. If there is no evidence of certificate status checking being used, this is a finding.

Remediation:

Configure the operating system to implement certificate status checking for multifactor authentication.

Review the "/etc/sssd/sssd.conf" file to determine if the system is configured to prevent OCSP or certificate verification.

Add the following line to the "/etc/sssd/sssd.conf" file:

```
certificate_verification = ocsp_dgst=sha1
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

`certificate_verification = ocsp_dgst=sha1`

If the `certificate_verification` line is missing from the [sssd] section, or is missing "`ocsp_dgst=sha1`", ask the administrator to indicate what type of multifactor authentication is being utilized and how the system implements certificate status checking. If there is no evidence of certificate status checking being used, this is a finding.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230274

Rule ID: SV-230274r743945_rule

STIG ID: RHEL-08-010400

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●

1.22 Ensure the operating system accepts PIV credentials (Automated)

Profile Applicability:

- STIG

Description:

The operating system must accept Personal Identity Verification (PIV) credentials.

Rationale:

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

The DoD has mandated the use of the Common Access Card (CAC) to support identity management and personal authentication for systems covered under Homeland Security Presidential Directive (HSPD) 12, as well as making the CAC a primary component of layered protection for national security systems.

Audit:

Verify the operating system accepts PIV credentials.

Check that the "opensc" package is installed on the system with the following command:

```
# dnf list installed opensc  
opensc.x86_64 0.19.0-5.el8 @anaconda
```

Check that "opensc" accepts PIV cards with the following command:

```
# opensc-tool --list-drivers | grep -i piv  
PIV-II Personal Identity Verification Card
```

If the "opensc" package is not installed and the "opensc-tool" driver list does not include "PIV-II", this is a finding.

Remediation:

Configure the operating system to accept PIV credentials.

Install the "opensc" package using the following command:

```
# dnf install opensc
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230275

Rule ID: SV-230275r627750_rule

STIG ID: RHEL-08-010410

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.23 Ensure the NX (no-execution) bit flag is set on the system (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement non-executable data to protect its memory from unauthorized code execution.

Rationale:

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Examples of attacks are buffer overflow attacks.

Audit:

Verify the NX (no-execution) bit flag is set on the system.

Check that the no-execution bit flag is set with the following commands:

```
# dmesg | grep NX  
[ 0.000000] NX (Execute Disable) protection: active
```

If "dmesg" does not show "NX (Execute Disable) protection" active, check the cpufreq settings with the following command:

```
# less /proc/cpuinfo | grep -i flags  
flags : fpu vme de pse tsc ms nx rdtscp lm constant_tsc
```

If "flags" does not contain the "nx" flag, this is a finding.

Remediation:

The NX bit execute protection must be enabled in the system BIOS.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230276

Rule ID: SV-230276r627750_rule

STIG ID: RHEL-08-010420

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.24 Ensure kernel page-table isolation is enabled (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enable mitigations against processor-based vulnerabilities.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled. Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is to not have the capability installed.

Kernel page-table isolation is a kernel feature that mitigates the Meltdown security vulnerability and hardens the kernel against attempts to bypass kernel address space layout randomization (KASLR).

Audit:

Verify the operating system enables kernel page-table isolation with the following commands:

```
# grub2-editenv - list | grep pti  
  
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto  
resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb  
quiet fips=1 audit=1 audit_backlog_limit=8192 pti=on boot=UUID=8d171156-cd61-  
421c-ba41-1c021ac29e82
```

If the "pti" entry does not equal "on", is missing, or the line is commented out, this is a finding.

Check that kernel page-table isolation is enabled by default to persist in kernel updates:

```
# grep audit /etc/default/grub  
  
GRUB_CMDLINE_LINUX="pti=on"
```

If "pti" is not set to "on", is missing or commented out, this is a finding.

Remediation:

Configure the operating system to enable kernel page-table isolation with the following command:

```
# grubby --update-kernel=ALL --args="pti=on"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="pti=on"
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230491

Rule ID: SV-230491r627750_rule

STIG ID: RHEL-08-040004

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.25 Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable access to network bpf syscall from unprivileged processes.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Audit:

Verify the operating system prevents privilege escalation thru the kernel by disabling access to the bpf syscall with the following commands:

```
# sysctl kernel.unprivileged_bpf_disabled  
kernel.unprivileged_bpf_disabled = 1
```

If the returned line does not have a value of "1", or a line is not returned, this is a finding.

Remediation:

Configure the operating system to prevent privilege escalation thru the kernel by disabling access to the bpf syscall by adding the following line to a file in the "/etc/sysctl.d" directory:

```
kernel.unprivileged_bpf_disabled = 1
```

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
# sysctl --system
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230545

Rule ID: SV-230545r627750_rule

STIG ID: RHEL-08-040281

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

1.26 Ensure the operating system restricts usage of ptrace to descendant processes (Automated)

Profile Applicability:

- STIG

Description:

The operating system must restrict usage of ptrace to descendant processes.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Audit:

Verify the operating system restricts usage of ptrace to descendant processes with the following commands:

```
# sysctl kernel.yama.ptrace_scope  
kernel.yama.ptrace_scope = 1
```

If the returned line does not have a value of "1", or a line is not returned, this is a finding.

Remediation:

Configure the operating system to restrict usage of ptrace to descendant processes by adding the following line to a file in the "/etc/sysctl.d" directory:

```
kernel.yama.ptrace_scope = 1
```

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
# sysctl --system
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230546

Rule ID: SV-230546r627750_rule

STIG ID: RHEL-08-040282

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

1.27 Ensure the operating system restricts exposed kernel pointer addresses access (Automated)

Profile Applicability:

- STIG

Description:

The operating system must restrict exposed kernel pointer addresses access.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Audit:

Verify the operating system restricts exposed kernel pointer addresses access with the following commands:

```
# sysctl kernel.kptr_restrict  
kernel.kptr_restrict = 1
```

If the returned line does not have a value of "1", or a line is not returned, this is a finding.

Remediation:

Configure the operating system to restrict exposed kernel pointer addresses access by adding the following line to a file in the "/etc/sysctl.d" directory:

```
kernel.kptr_restrict = 1
```

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
# sysctl --system
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230547

Rule ID: SV-230547r627750_rule

STIG ID: RHEL-08-040283

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.28 Ensure the operating system disables the ability to load the firewire-core kernel module (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable IEEE 1394 (FireWire) Support.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

The IEEE 1394 (FireWire) is a serial bus standard for high-speed real-time communication. Disabling FireWire protects the system against exploitation of any flaws in its implementation.

Audit:

Verify the operating system disables the ability to load the firewire-core kernel module.

```
# grep -ri firewire-core /etc/modprobe.d/* | grep -i "/bin/true"  
install firewire-core /bin/true
```

If the command does not return any output, or the line is commented out, and use of the firewire-core protocol is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify the operating system disables the ability to use the firewire-core kernel module. Check to see if the firewire-core kernel module is disabled with the following command:

```
# grep -ri firewire-core /etc/modprobe.d/* | grep -i "blacklist"  
blacklist firewire-core
```

If the command does not return any output or the output is not "blacklist firewire-core", and use of the firewire-core kernel module is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the operating system to disable the ability to use the firewire-core kernel module.

Add or update the following lines in the file "/etc/modprobe.d/blacklist.conf":

```
install firewire-core /bin/true  
blacklist firewire-core
```

Reboot the system for the settings to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230499

Rule ID: SV-230499r627750_rule

STIG ID: RHEL-08-040026

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.29 Ensure the operating system disables the ability to load the USB Storage kernel module (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured to disable USB mass storage.

Rationale:

USB mass storage permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163

Audit:

Verify the operating system disables the ability to load the USB Storage kernel module.

```
# grep -r usb-storage /etc/modprobe.d/* | grep -i "/bin/true"  
install usb-storage /bin/true
```

If the command does not return any output, or the line is commented out, and use of USB Storage is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify the operating system disables the ability to use USB mass storage devices.

Check to see if USB mass storage is disabled with the following command:

```
# grep usb-storage /etc/modprobe.d/* | grep -i "blacklist"  
blacklist usb-storage
```

If the command does not return any output or the output is not "blacklist usb-storage", and use of USB storage devices is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the operating system to disable the ability to use the USB Storage kernel module. Create a file under "/etc/modprobe.d" with the following command:

```
# touch /etc/modprobe.d/usb-storage.conf
```

Add the following line to the created file:

```
install usb-storage /bin/true
```

Configure the operating system to disable the ability to use USB mass storage devices.

```
# vi /etc/modprobe.d/blacklist.conf
```

Add or update the line:

```
blacklist usb-storage
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230503

Rule ID: SV-230503r627750_rule

STIG ID: RHEL-08-040080

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.30 Ensure the operating system disables the use of user namespaces (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable the use of user namespaces.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

User namespaces are used primarily for Linux container. The value 0 disallows the use of user namespaces. When containers are not in use, namespaces should be disallowed. When containers are deployed on a system, the value should be set to a large non-zero value. The default value is 7182.

Audit:

Verify the operating system disables the use of user namespaces with the following commands:

Note: User namespaces are used primarily for Linux containers. If containers are in use, this requirement is not applicable.

```
# sysctl user.max_user_namespaces
user.max_user_namespaces = 0
```

If the returned line does not have a value of "0", or a line is not returned, this is a finding.

Remediation:

Configure the operating system to disable the use of user namespaces by adding the following line to a file in the "/etc/sysctl.d" directory:

Note: User namespaces are used primarily for Linux containers. If containers are in use, this requirement is not applicable.

```
user.max_user_namespaces = 0
```

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
# sysctl --system
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230548

Rule ID: SV-230548r627750_rule

STIG ID: RHEL-08-040284

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.31 Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service (Automated)

Profile Applicability:

- STIG

Description:

The operating system must have the packages required to use the hardware random number generator entropy gatherer service.

Rationale:

The most important characteristic of a random number generator is its randomness, namely its ability to deliver random numbers that are impossible to predict. Entropy in computer security is associated with the unpredictability of a source of randomness. The random source with high entropy tends to achieve a uniform distribution of random values. Random number generators are one of the most important building blocks of cryptosystems.

The rngd service feeds random data from hardware device to kernel random device. Quality (non-predictable) random number generation is important for several security functions (i.e., ciphers).

Audit:

Check that the operating system has the packages required to enabled the hardware random number generator entropy gatherer service with the following command:

```
# dnf list installed rng-tools
rng-tools.x86_64 6.8-3.el8 @anaconda
```

If the "rng-tools" package is not installed, this is a finding.

Remediation:

Install the packages required to enabled the hardware random number generator entropy gatherer service with the following command:

```
# dnf install rng-tools
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244527

Rule ID: SV-244527r743830_rule

STIG ID: RHEL-08-010472

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.32 Ensure the "tmux" package installed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must have the tmux package installed.

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, the operating system needs to provide users with the ability to manually invoke a session lock so users can secure their session if it is necessary to temporarily vacate the immediate physical vicinity.

Tmux is a terminal multiplexer that enables a number of terminals to be created, accessed, and controlled from a single screen. Red Hat endorses tmux as the recommended session controlling package.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Verify the operating system has the "tmux" package installed, by running the following command:

```
# dnf list installed tmux  
tmux.x86_64 2.7-1.el8 @repository
```

If "tmux" is not installed, this is a finding.

Remediation:

Configure the operating system to enable a user to initiate a session lock via tmux.

Install the "tmux" package, if it is not already installed, by running the following command:

```
# dnf install tmux
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244537

Rule ID: SV-244537r743860_rule

STIG ID: RHEL-08-020039

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.33 Ensure the operating system enables hardening for the BPF JIT (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enable hardening for the Berkeley Packet Filter Just-in-time compiler.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Enabling hardening for the Berkeley Packet Filter (BPF) Just-in-time (JIT) compiler aids in mitigating JIT spraying attacks. Setting the value to "2" enables JIT hardening for all users.

Audit:

Verify the operating system enables hardening for the BPF JIT with the following commands:

```
# sysctl net.core.bpf_jit_harden  
net.core.bpf_jit_harden = 2
```

If the returned line does not have a value of "2", or a line is not returned, this is a finding.

Remediation:

Configure the operating system to enable hardening for the BPF JIT compiler by adding the following line to a file in the "/etc/sysctl.d" directory:

```
net.core.bpf_jit_harden = 2
```

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
# sysctl --system
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244554

Rule ID: SV-244554r743911_rule

STIG ID: RHEL-08-040286

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.34 Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool (Automated)

Profile Applicability:

- STIG

Description:

The Endpoint Security for Linux Threat Prevention tool must be implemented.

Rationale:

Adding endpoint security tools can provide the capability to automatically take actions in response to malicious behavior, which can provide additional agility in reacting to network threats. These tools also often include a reporting capability to provide network awareness of the system, which may not otherwise exist in an organization's systems management regime.

Audit:

Per OPORD 16-0080, the preferred endpoint security tool is McAfee Endpoint Security for Linux (ENSL) in conjunction with SELinux.

Procedure:

Check that the following package has been installed:

```
# rpm -qa | grep -i mcafeftp
```

If the "mcafeftp" package is not installed, this is a finding.

Verify that the daemon is running:

```
# ps -ef | grep -i mfetpd
```

If the daemon is not running, this is a finding.

Remediation:

Install and enable the latest McAfee ENSLTP package.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-245540

Rule ID: SV-245540r754730_rule

STIG ID: RHEL-08-010001

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

2 Services

While applying system updates and patches helps correct known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to disable all services that are not required for normal system operation. This prevents the exploitation of vulnerabilities discovered at a later date. If a service is not enabled, it cannot be exploited. The actions in this section of the document provide guidance on some services which can be safely disabled and under which circumstances, greatly reducing the number of possible threats to the resulting system. Additionally, some services which should remain enabled but with secure configuration are covered as well as insecure service clients.

2.1 inetd Services

inetd is a super-server daemon that provides internet services and passes connections to configured services. While not commonly used inetd and any unneeded inetd based services should be disabled if possible.

2.1.1 Ensure xinetd is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The eXtended InterNET Daemon (`xinetd`) is an open source super daemon that replaced the original `inetd` daemon. The `xinetd` daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests.

Rationale:

If there are no `xinetd` services required, it is recommended that the package be removed.

Audit:

Run the following command to verify `xinetd` is not installed:

```
# rpm -q xinetd  
package xinetd is not installed
```

Remediation:

Run the following command to remove `xinetd`:

```
# dnf remove xinetd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2 Special Purpose Services

This section describes services that are installed on systems that specifically need to run these services. If any of these services are not required, it is recommended that they be disabled or deleted from the system to reduce the potential attack surface.

2.2.1 Time Synchronization

It is recommended that physical systems and virtual guests lacking direct access to the physical host's clock be configured to synchronize their time using chrony.

2.2.1.1 Ensure time synchronization is in use (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of servers and having all systems synchronize their clocks to them.

Rationale:

Time synchronization is important to support time sensitive security mechanisms like Kerberos and also ensures log files have consistent time records across the enterprise, which aids in forensic investigations.

Audit:

On physical systems or virtual systems where host based time synchronization is not available verify that chrony is installed.

Run the following command to verify that chrony is installed

```
# rpm -q chrony  
chrony-<VERSION>
```

On virtual systems where host based time synchronization is available consult your virtualization software documentation and verify that host based synchronization is in use.

Remediation:

On physical systems or virtual systems where host based time synchronization is not available install chrony:

Run the following command to install chrony:

```
# dnf install chrony
```

On virtual systems where host based time synchronization is available consult your virtualization software documentation and setup host based synchronization.

Additional Information:

systemd-timesyncd is part of systemd. Some versions of systemd have been compiled without systemd-timesyncd. On these distributions, chrony or NTP should be used instead of systemd-timesyncd.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.2.1.2 Ensure chrony is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`chrony` is a daemon which implements the Network Time Protocol (NTP) and is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on `chrony` can be found at <http://chrony.tuxfamily.org/>. `chrony` can be configured to be a client and/or a server.

Rationale:

If `chrony` is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

This recommendation only applies if `chrony` is in use on the system.

Audit:

Run the following command and verify remote server is configured properly:

```
# grep -E "^(server|pool)" /etc/chrony.conf  
server <remote-server>
```

Multiple servers may be configured.

Run the following command and verify the first field for the `chronyd` process is `chrony`:

```
# ps -ef | grep chronyd  
chrony      491      1  0 20:32 ?          00:00:00 /usr/sbin/chronyd
```

Remediation:

Add or edit server or pool lines to `/etc/chrony.conf` as appropriate:

```
server <remote-server>
```

Configure `chrony` to run as the `chrony` user

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.2.1.3 Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server (Automated)

Profile Applicability:

- STIG

Description:

must securely compare internal information system clocks at least every 24 hours with a server synchronized to an authoritative time source, such as the United States Naval Observatory (USNO) time servers, or a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network. Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis.

Time stamps generated by the operating system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

RHEL 8 operating systems utilize the "timedatectl" command to view the status of the "systemd-timesyncd.service". The "timedatectl" status will display the local time, UTC, and the offset from UTC.

Note that USNO offers authenticated NTP service to DoD and U.S. Government agencies operating on the NIPR and SIPR networks. Visit <https://www.usno.navy.mil/USNO/time/ntp/dod-customers> for more information.

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144, SRG-OS-000359-GPOS-00146

Audit:

Verify the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server with the following commands:

```
# grep maxpoll /etc/chrony.conf  
server 0.us.pool.ntp.mil iburst maxpoll 16
```

If the "maxpoll" option is set to a number greater than 16 or the line is commented out, this is a finding.

Verify the "chrony.conf" file is configured to an authoritative DoD time source by running the following command:

```
# grep -i server /etc/chrony.conf  
server 0.us.pool.ntp.mil
```

If the parameter "server" is not set or is not set to an authoritative DoD time source, this is a finding.

Remediation:

Configure the operating system to securely compare internal information system clocks at least every 24 hours with an NTP server by adding/modifying the following line in the /etc/chrony.conf file.

```
server [ntp.server.name] iburst maxpoll 16
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230484

Rule ID: SV-230484r627750_rule

STIG ID: RHEL-08-030740

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.2.1.4 Ensure the operating system disables the chrony daemon from acting as a server (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable the chrony daemon from acting as a server.

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Minimizing the exposure of the server functionality of the chrony daemon diminishes the attack surface.

RHEL 8 operating systems utilize the "timedatectl" command to view the status of the "systemd-timesyncd.service". The "timedatectl" status will display the local time, UTC, and the offset from UTC.

Note that USNO offers authenticated NTP service to DoD and U.S. Government agencies operating on the NIPR and SIPR networks. Visit <https://www.usno.navy.mil/USNO/time/ntp/dod-customers> for more information.

Audit:

Verify the operating system disables the chrony daemon from acting as a server with the following command:

```
# grep -w 'port' /etc/chrony.conf  
port 0
```

If the "port" option is not set to "0", is commented out or missing, this is a finding.

Remediation:

Configure the operating system to disable the chrony daemon from acting as a server by adding/modifying the following line in the "/etc/chrony.conf" file.

```
port 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230485

Rule ID: SV-230485r627750_rule

STIG ID: RHEL-08-030741

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.1.5 Ensure the operating system disables network management of the chrony daemon (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable network management of the chrony daemon.

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Not exposing the management interface of the chrony daemon on the network diminishes the attack space.

RHEL 8 operating systems utilize the "timedatectl" command to view the status of the "systemd-timesyncd.service". The "timedatectl" status will display the local time, UTC, and the offset from UTC.

Note that USNO offers authenticated NTP service to DoD and U.S. Government agencies operating on the NIPR and SIPR networks. Visit <https://www.usno.navy.mil/USNO/time/ntp/dod-customers> for more information.

Audit:

Verify the operating system disables network management of the chrony daemon with the following command:

```
# grep -w 'cmdport' /etc/chrony.conf  
cmdport 0
```

If the "cmdport" option is not set to "0", is commented out or missing, this is a finding.

Remediation:

Configure the operating system disable network management of the chrony daemon by adding/modifying the following line in the /etc/chrony.conf file.

```
cmdport 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230486

Rule ID: SV-230486r627750_rule

STIG ID: RHEL-08-030742

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.2 Ensure X Window System is not installed (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The X Window System provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Windows system is typically used on workstations where users login, but not on servers where users typically do not login.

Rationale:

Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.

Impact:

Many Linux systems run applications which require a Java runtime. Some Linux Java packages have a dependency on specific X Windows xorg-x11-fonts. One workaround to avoid this dependency is to use the "headless" Java packages for your specific Java runtime, if provided by your distribution.

Audit:

Run the following command to Verify X Windows System is not installed.

```
# rpm -qa xorg-x11-server-*
```

Remediation:

Run the following command to remove the X Windows System packages.

```
# dnf remove xorg-x11-server-*
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

2.2.3 Ensure rsync service is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsynccd` service can be used to synchronize files between systems over network links.

Rationale:

The `rsynccd` service presents a security risk as it uses unencrypted protocols for communication.

Audit:

Run the following command to verify `rsynccd` is not enabled:

```
# systemctl is-enabled rsynccd  
disabled
```

Verify result is not "enabled"

Remediation:

Run the following command to disable `rsynccd`:

```
# systemctl --now disable rsynccd
```

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

On some distributions the rsync service is known as `rsync`, not `rsynccd`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.4 Ensure Avahi Server is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine.

Rationale:

Automatic discovery of network services is not normally required for system functionality. It is recommended to disable the service to reduce the potential attack surface.

Audit:

Run the following command to verify `avahi-daemon.socket` is not enabled:

```
# systemctl is-enabled avahi-daemon.socket  
disabled
```

Verify result is not "enabled".

Run the following command to verify `avahi-daemon.serivce` is not enabled:

```
# systemctl is-enabled avahi-daemon  
disabled
```

Verify result is not "enabled".

Remediation:

Run the following commands to disable `avahi-daemon.socket` and `avahi-daemon.service`:

```
# systemctl --now disable avahi-daemon.socket  
# systemctl --now disable avahi-daemon.service
```

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.5 Ensure SNMP Server is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

Rationale:

The SNMP server can communicate using SNMP v1, which transmits data in the clear and does not require authentication to execute commands. Unless absolutely necessary, it is recommended that the SNMP service not be used. If SNMP is required the server should be configured to disallow SNMP v1.

Audit:

Run the following command to verify `snmpd` is not enabled:

```
# systemctl is-enabled snmpd  
disabled
```

Verify result is not "enabled"

Remediation:

Run the following command to disable `snmpd`:

```
# systemctl --now disable snmpd
```

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.6 Ensure HTTP Proxy Server is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Squid is a standard proxy server used in many distributions and environments.

Rationale:

If there is no need for a proxy server, it is recommended that the squid proxy be deleted to reduce the potential attack surface.

Audit:

Run the following command to verify `squid` is not enabled:

```
# systemctl is-enabled squid  
disabled
```

Verify result is not "enabled"

Remediation:

Run the following command to disable `squid`:

```
# systemctl --now disable squid
```

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.7 Ensure Samba is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Server Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems.

Rationale:

If there is no need to mount directories and file systems to Windows systems, then this service can be deleted to reduce the potential attack surface.

Audit:

Run the following command to verify `smb` is not enabled:

```
# systemctl is-enabled smb  
disabled
```

Verify result is not "enabled".

Remediation:

Run the following command to disable `smb`:

```
# systemctl --now disable smb
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.8 Ensure IMAP and POP3 server is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`dovecot` is an open source IMAP and POP3 server for Linux based systems.

Rationale:

Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the service be deleted to reduce the potential attack surface.

Audit:

Run the following command to verify `dovecot` is not enabled:

```
# systemctl is-enabled dovecot  
disabled
```

Verify result is not "enabled".

Remediation:

Run the following command to disable `dovecot`:

```
# systemctl --now disable dovecot
```

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Several IMAP/POP3 servers exist and can use other service names. `courier-imap` and `cyrus-imap` are example services that provide a mail server. These and other services should also be audited.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.9 Ensure HTTP server is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

HTTP or web servers provide the ability to host web site content.

Rationale:

Unless there is a need to run the system as a web server, it is recommended that the package be deleted to reduce the potential attack surface.

Audit:

Run the following command to verify `httpd` is not enabled:

```
# systemctl is-enabled httpd  
disabled
```

Verify result is not "enabled".

Remediation:

Run the following command to disable `httpd`:

```
# systemctl --now disable httpd
```

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Several `httpd` servers exist and can use other service names. `apache`, `apache2`, `lighttpd`, and `nginx` are example services that provide an HTTP server. These and other services should also be audited.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.10 Ensure FTP Server is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files.

Rationale:

FTP does not protect the confidentiality of data or authentication credentials. It is recommended SFTP be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be deleted to reduce the potential attack surface.

Audit:

Run the following command to verify vsftpd is not enabled:

```
# systemctl is-enabled vsftpd  
disabled
```

Verify result is not "enabled".

Remediation:

Run the following command to disable vsftpd :

```
# systemctl --now disable vsftpd
```

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Additional FTP servers also exist and should be audited.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.11 Ensure DNS Server is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network.

Rationale:

Unless a system is specifically designated to act as a DNS server, it is recommended that the package be deleted to reduce the potential attack surface.

Audit:

Run the following command to verify `named` is not enabled:

```
# systemctl is-enabled named  
disabled
```

Verify result is not "enabled".

Remediation:

Run the following command to disable `named`:

```
# systemctl --now disable named
```

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.12 Ensure NFS is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network.

Rationale:

If the system does not export NFS shares, it is recommended that the NFS be disabled to reduce the remote attack surface.

Audit:

Run the following command to verify the `nfs-server` is not enabled:

```
# systemctl is-enabled nfs-server  
disabled
```

Verify result is not "enabled".

Remediation:

Run the following commands to disable the `nfs-server`:

```
# systemctl --now disable nfs-server
```

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.13 Ensure RPC is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The rpcbind service maps Remote Procedure Call (RPC) services to the ports on which they listen. RPC processes notify rpcbind when they start, registering the ports they are listening on and the RPC program numbers they expect to serve. The client system then contacts rpcbind on the server with a particular RPC program number. The rpcbind service redirects the client to the proper port number so it can communicate with the requested service.

Rationale:

If the system does not require rpc based services, it is recommended that rpcbind be disabled to reduce the remote attack surface.

Impact:

Because RPC-based services rely on rpcbind to make all connections with incoming client requests, rpcbind must be available before any of these services start

Audit:

Run the following command to verify rpcbind is not enabled:

```
# systemctl is-enabled rpcbind  
disabled
```

Verify result is not "enabled".

Remediation:

Run the following commands to disable rpcbind:

```
# systemctl --now disable rpcbind
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.14 Ensure LDAP server is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

Rationale:

If the system will not need to act as an LDAP server, it is recommended that the software be disabled to reduce the potential attack surface.

Audit:

Run the following commands to verify `slapd` is not enabled:

```
# systemctl is-enabled slapd  
disabled
```

Verify result is not "enabled".

Remediation:

Run the following command to disable `slapd`:

```
# systemctl --now disable slapd
```

References:

1. For more detailed documentation on OpenLDAP, go to the project homepage at <http://www.openldap.org>.

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.15 Ensure DHCP Server is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses.

Rationale:

Unless a system is specifically set up to act as a DHCP server, it is recommended that this service be deleted to reduce the potential attack surface.

Audit:

Run the following command to verify `dhcpcd` is not enabled:

```
# systemctl is-enabled dhcpcd  
disabled
```

Verify result is not "enabled".

Remediation:

Run the following command to disable `dhcpcd`:

```
# systemctl --now disable dhcpcd
```

References:

1. More detailed documentation on DHCP is available at <http://www.isc.org/software/dhcp>.

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.16 Ensure the telnet-server package is not installed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not have the telnet-server package installed.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled. Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is to not have the capability installed.

The telnet service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service, the privileged user password could be compromised.

Audit:

Check to see if the telnet-server package is installed with the following command:

```
# yum list installed telnet-server
```

If the telnet-server package is installed, this is a finding.

Remediation:

Configure the operating system to disable non-essential capabilities by removing the telnet-server package from the system with the following command:

```
# yum remove telnet-server
```

Additional Information:

Vul ID: V-230487

Rule ID: SV-230487r627750_rule

STIG ID: RHEL-08-040000

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.17 Ensure CUPS is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability.

Rationale:

If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be disabled to reduce the potential attack surface.

Impact:

Disabling CUPS will prevent printing from the system, a common task for workstation systems.

Audit:

Run the following command to verify `cups` is not enabled:

```
# systemctl is-enabled cups  
disabled
```

Verify result is not "enabled".

Remediation:

Run the following command to disable `cups`:

```
# systemctl --now disable cups
```

References:

1. More detailed documentation on CUPS is available at the project homepage at <http://www.cups.org>.

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.18 Ensure NIS Server is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files.

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be disabled and other, more secure services be used

Audit:

Run the following command to verify `ypserv` is not enabled:

```
# systemctl is-enabled ypserv  
disabled
```

Verify result is not "enabled"

Remediation:

Run the following command to disable `ypserv`:

```
# systemctl --now disable ypserv
```

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.19 Ensure mail transfer agent is configured for local-only mode (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.

Rationale:

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

Audit:

Run the following command to verify that the MTA is not listening on any non-loopback address (127.0.0.1 or ::1)

Nothing should be returned

```
# ss -lntu | grep -E ':25\s' | grep -E -v '\s(127.0.0.1|::1):25\s'
```

Remediation:

Edit /etc/postfix/main.cf and add the following line to the RECEIVING MAIL section. If the line already exists, change it to look like the line below:

```
inet_interfaces = loopback-only
```

Run the following command to restart postfix

```
# systemctl restart postfix
```

Additional Information:

This recommendation is designed around the postfix mail server, depending on your environment you may have an alternative MTA installed such as sendmail. If this is the case consult the documentation for your installed MTA to configure the recommended state.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.20 Ensure the operating system has enabled the hardware random number generator entropy gatherer service (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enable the hardware random number generator entropy gatherer service.

Rationale:

The most important characteristic of a random number generator is its randomness, namely its ability to deliver random numbers that are impossible to predict. Entropy in computer security is associated with the unpredictability of a source of randomness. The random source with high entropy tends to achieve a uniform distribution of random values. Random number generators are one of the most important building blocks of cryptosystems.

The rngd service feeds random data from hardware device to kernel random device. Quality (non-predictable) random number generation is important for several security functions (i.e., ciphers).

Audit:

Check that the operating system has enabled the hardware random number generator entropy gatherer service.

Verify the rngd service is enabled and active with the following commands:

```
# systemctl is-enabled rngd  
enabled  
  
# systemctl is-active rngd  
active
```

If the service is not "enable and "active", this is a finding.

Remediation:

Start the rngd service, and enable the rngd service with the following commands:

```
# systemctl start rngd.service  
# systemctl enable rngd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230285

Rule ID: SV-230285r627750_rule

STIG ID: RHEL-08-010471

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.2.21 Ensure automated bug reporting tools are not installed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not have any automated bug reporting tools installed.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled. Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is to not have the capability installed.

Audit:

Check to see if any automated bug reporting packages are installed with the following command:

```
# dnf list installed abrt*
```

If any automated bug reporting package is installed, this is a finding.

Remediation:

Configure the operating system to disable non-essential capabilities by removing automated bug reporting packages from the system with the following command:

```
# dnf remove abrt*
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230488

Rule ID: SV-230488r627750_rule

STIG ID: RHEL-08-040001

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.22 Ensure the sendmail package is not installed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not have the sendmail package installed.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is to not have the capability installed.

Audit:

Check to see if the sendmail package is installed with the following command:

```
# dnf list installed sendmail
```

If the sendmail package is installed, this is a finding.

Remediation:

Configure the operating system to disable non-essential capabilities by removing the sendmail package from the system with the following command:

```
# dnf remove sendmail
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230489

Rule ID: SV-230489r627750_rule

STIG ID: RHEL-08-040002

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.23 Ensure the rsh-server package is not installed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not have the rsh-server package installed.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The rsh-server service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session and has very weak authentication.

If a privileged user were to log on using this service, the privileged user password could be compromised.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000074-GPOS-00042

Audit:

Check to see if the rsh-server package is installed with the following command:

```
# dnf list installed rsh-server
```

If the rsh-server package is installed, this is a finding.

Remediation:

Configure the operating system to disable non-essential capabilities by removing the rsh-server package from the system with the following command:

```
# dnf remove rsh-server
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230492

Rule ID: SV-230492r627750_rule

STIG ID: RHEL-08-040010

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.24 Ensure a camera is not installed (Manual)

Profile Applicability:

- STIG

Description:

The operating system must cover or disable the built-in or attached camera when not in use.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Failing to disconnect from collaborative computing devices (i.e., cameras) can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session helps to ensure participants actually carry out the disconnect activity without having to go through complex and tedious procedures.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Audit:

If the device or operating system does not have a camera installed, this requirement is not applicable.

This requirement is not applicable to mobile devices (smartphones and tablets), where the use of the camera is a local AO decision.

This requirement is not applicable to dedicated VTC suites located in approved VTC locations that are centrally managed.

For an external camera, if there is not a method for the operator to manually disconnect the camera at the end of collaborative computing sessions, this is a finding.

For a built-in camera, the camera must be protected by a camera cover (e.g., laptop camera cover slide) when not in use. If the built-in camera is not protected with a camera cover, or is not physically disabled, this is a finding.

If the camera is not disconnected, covered, or physically disabled, determine if it is being disabled via software with the following commands:

Determine if the camera is disabled via blacklist with the following command:

```
# grep blacklist /etc/modprobe.d/*
/etc/modprobe.d/blacklist.conf:blacklist uvcvideo
```

Determine if a camera driver is in use with the following command:

```
# dmesg | grep -i video

[ 44.630131] ACPI: Video Device [VGA]
[ 46.655714] input: Video Bus as
/devices/LNXSYSTEM:00/LNXSYBUS:00/LNXVIDEO:00/input/input7
[ 46.670133] videodev: Linux video capture interface: v2.00
[ 47.226424] uvcvideo: Found UVC 1.00 device WebCam (0402:7675)
[ 47.235752] usbcore: registered new interface driver uvcvideo
[ 47.235756] USB Video Class driver (1.1.1)
```

If the camera driver blacklist is missing, a camera driver is determined to be in use, and the collaborative computing device has not been authorized for use, this is a finding.

Remediation:

Configure the operating system to disable the built-in or attached camera when not in use.

First determine the driver being used by the camera with the following command:

```
# dmesg | grep -i video

[ 44.630131] ACPI: Video Device [VGA]
[ 46.655714] input: Video Bus as
/devices/LNXSYSTM:00/LNXSYBUS:00/LNXVIDEO:00/input/input7
[ 46.670133] videodev: Linux video capture interface: v2.00
[ 47.226424] uvcvideo: Found UVC 1.00 device WebCam (0402:7675)
[ 47.235752] usbcore: registered new interface driver uvcvideo
[ 47.235756] USB Video Class driver (1.1.1)
```

Next, build or modify the "/etc/modprobe.d/blacklist.conf" file by using the following example:

```
##Disable WebCam
blacklist uvcvideo
```

Reboot the system for the settings to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230493

Rule ID: SV-230493r627750_rule

STIG ID: RHEL-08-040020

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.25 Ensure the operating system is configured to mask the debug-shell systemd service (Automated)

Profile Applicability:

- STIG

Description:

The debug-shell systemd service must be disabled.

Rationale:

The debug-shell requires no authentication and provides root privileges to anyone who has physical access to the machine. While this feature is disabled by default, masking it adds an additional layer of assurance that it will not be enabled via a dependency in systemd. This also prevents attackers with physical access from trivially bypassing security on the machine through valid troubleshooting configurations and gaining root access when the system is rebooted.

Audit:

Verify the operating system is configured to mask the debug-shell systemd service with the following command:

```
# systemctl status debug-shell.service  
  
debug-shell.service  
Loaded: masked (Reason: Unit debug-shell.service is masked.)  
Active: inactive (dead)
```

If the "debug-shell.service" is loaded and not masked, this is a finding.

Remediation:

Configure the system to mask the debug-shell systemd service with the following command:

```
# systemctl mask debug-shell.service  
  
Created symlink /etc/systemd/system/debug-shell.service -> /dev/null
```

Reload the daemon to take effect.

```
# systemctl daemon-reload
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230532

Rule ID: SV-230532r627750_rule

STIG ID: RHEL-08-040180

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.26 Ensure a TFTP server has not been installed on the system (Automated)

Profile Applicability:

- STIG

Description:

The Trivial File Transfer Protocol (TFTP) server package must not be installed if not required for operational support.

Rationale:

If TFTP is required for operational support (such as the transmission of router configurations) its use must be documented with the Information System Security Officer (ISSO), restricted to only authorized personnel, and have access control rules established.

Audit:

Verify a TFTP server has not been installed on the system with the following command:

```
# dnf list installed tftp-server
tftp-server.x86_64 5.2-24.el8
```

If TFTP is installed and the requirement for TFTP is not documented with the ISSO, this is a finding.

Remediation:

Remove the TFTP package from the system with the following command:

```
# dnf remove tftp-server
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230533

Rule ID: SV-230533r627750_rule

STIG ID: RHEL-08-040190

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.27 Ensure the operating system is configured to prevent unrestricted mail relaying (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured to prevent unrestricted mail relaying.

Rationale:

If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending spam or other unauthorized activity.

Audit:

Verify the system is configured to prevent unrestricted mail relaying.
Determine if "postfix" is installed with the following commands:

```
# dnf list installed postfix  
postfix.x86_64 2:3.3.1-9.el8
```

If postfix is not installed, this is Not Applicable.

If postfix is installed, determine if it is configured to reject connections from unknown or untrusted networks with the following command:

```
# postconf -n smtpd_client_restrictions  
smtpd_client_restrictions = permit_mynetworks, reject
```

If the "smtpd_client_restrictions" parameter contains any entries other than "permit_mynetworks" and "reject", this is a finding.

Remediation:

If "postfix" is installed, modify the "/etc/postfix/main.cf" file to restrict client connections to the local network with the following command:

```
# postconf -e 'smtpd_client_restrictions = permit_mynetworks,reject'
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230550

Rule ID: SV-230550r627750_rule

STIG ID: RHEL-08-040290

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.28 Ensure the TFTP daemon is configured to operate in secure mode (Automated)

Profile Applicability:

- STIG

Description:

If the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon must be configured to operate in secure mode.

Rationale:

Restricting TFTP to a specific directory prevents remote users from copying, transferring, or overwriting system files.

Audit:

Verify the TFTP daemon is configured to operate in secure mode with the following commands:

```
# dnf list installed tftp-server  
tftp-server.x86_64 x.x-x.el8
```

If a TFTP server is not installed, this is Not Applicable.

If a TFTP server is installed, check for the server arguments with the following command:

```
# grep server_args /etc/xinetd.d/tftp  
server_args = -s /var/lib/tftpboot
```

If the "server_args" line does not have a "-s" option, and a subdirectory is not assigned, this is a finding.

Remediation:

Configure the TFTP daemon to operate in secure mode by adding the following line to "/etc/xinetd.d/tftp" (or modify the line to have the required value):

```
server_args = -s /var/lib/tftpboot
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230557

Rule ID: SV-230557r627750_rule

STIG ID: RHEL-08-040350

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.2.29 Ensure an FTP server has not been installed on the system (Automated)

Profile Applicability:

- STIG

Description:

A File Transfer Protocol (FTP) server package must not be installed unless it is mission essential.

Rationale:

The FTP service provides an unencrypted remote access that does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service, the privileged user password could be compromised. SSH or other encrypted file transfer methods must be used in place of this service.

Audit:

Verify an FTP server has not been installed on the system with the following commands:

```
# dnf list installed *ftpd*
vsftpd.x86_64 3.0.3-28.el8 appstream
```

If an FTP server is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the FTP server package with the ISSO as an operational requirement or remove it from the system with the following command:

```
# dnf remove vsftpd
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230558

Rule ID: SV-230558r627750_rule

STIG ID: RHEL-08-040360

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.30 Ensure the gssproxy package has not been installed on the system (Automated)

Profile Applicability:

- STIG

Description:

The gssproxy package must not be installed unless it is mission essential.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The gssproxy package is a proxy for GSS API credential handling and could expose secrets on some networks. It is not needed for normal function of the OS.

Audit:

Verify the gssproxy package has not been installed on the system with the following commands:

```
# dnf list installed gssproxy  
gssproxy.x86_64 0.8.0-14.el8 @anaconda
```

If the gssproxy package is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the gssproxy package with the ISSO as an operational requirement or remove it from the system with the following command:

```
# dnf remove gssproxy
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230559

Rule ID: SV-230559r646887_rule

STIG ID: RHEL-08-040370

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.31 Ensure the iprutils package has not been installed on the system (Automated)

Profile Applicability:

- STIG

Description:

The iprutils package must not be installed unless it is mission essential.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The iprutils package provides a suite of utilities to manage and configure SCSI devices supported by the ipr SCSI storage device driver.

Audit:

Verify the iprutils package has not been installed on the system with the following commands:

```
# dnf list installed iprutils  
iprutils.x86_64 2.4.18.1-1.el8 @anaconda
```

If the iprutils package is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the iprutils package with the ISSO as an operational requirement or remove it from the system with the following command:

```
# dnf remove iprutils
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230560

Rule ID: SV-230560r627750_rule

STIG ID: RHEL-08-040380

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.32 Ensure the tuned package has not been installed on the system (Automated)

Profile Applicability:

- STIG

Description:

The tuned package must not be installed unless it is mission essential.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The tuned package contains a daemon that tunes the system settings dynamically. It does so by monitoring the usage of several system components periodically. Based on that information, components will then be put into lower or higher power savings modes to adapt to the current usage. The tuned package is not needed for normal OS operations.

Audit:

Verify the tuned package has not been installed on the system with the following commands:

```
# dnf list installed tuned
tuned.noarch 2.12.0-3.el8 @anaconda
```

If the tuned package is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the tuned package with the ISSO as an operational requirement or remove it from the system with the following command:

```
# dnf remove tuned
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230561

Rule ID: SV-230561r627750_rule

STIG ID: RHEL-08-040390

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.33 Ensure the krb5-server package has not been installed on the system (Automated)

Profile Applicability:

- STIG

Description:

The krb5-server package must not be installed.

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

RHEL 8 operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

Currently, Kerberos does not utilize FIPS 140-2 cryptography.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

Audit:

Verify the krb5-server package has not been installed on the system with the following commands:

If the system is a workstation or is utilizing krb5-server-1.17-18.el8.x86_64 or newer, this is Not Applicable

```
# dnf list installed krb5-server  
krb5-server.x86_64 1.17-9.el8 repository
```

If the krb5-server package is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the krb5-server package with the ISSO as an operational requirement or remove it from the system with the following command:

```
# dnf remove krb5-server
```

Additional Information:

Vul ID: V-237640

Rule ID: SV-237640r646890_rule

STIG ID: RHEL-08-010163

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.3 Service Clients

A number of insecure services exist. While disabling the servers prevents a local attack against these services, it is advised to remove their clients unless they are required.

Note: This should not be considered a comprehensive list of insecure service clients. You may wish to consider additions to those listed here for your environment.

2.3.1 Ensure NIS Client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client (`ypbind`) was used to bind a machine to an NIS server and receive the distributed configuration files.

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Audit:

Verify `ypbind` is not installed.

Run the following command:

```
# rpm -q ypbnd  
package ypbnd is not installed
```

Remediation:

Run the following command to Uninstall `ypbind`

```
# dnf remove ypbnd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

2.3.2 Ensure telnet client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `telnet` package contains the `telnet` client, which allows users to start connections to other systems via the telnet protocol.

Rationale:

The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The `ssh` package provides an encrypted session and stronger security and is included in most Linux distributions.

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Audit:

Verify `telnet` is not installed.

Run the following command:

```
# rpm -q telnet  
package telnet is not installed
```

Remediation:

Run the following command to uninstall `telnet`

```
# dnf remove telnet
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.			

2.3.3 Ensure LDAP client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

Rationale:

If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.

Impact:

Removing the LDAP client will prevent or inhibit using LDAP for authentication in your environment.

Audit:

Verify openldap-clients is not installed.

Run the following command:

```
# rpm -q openldap-clients  
package openldap-clients is not installed
```

Remediation:

Run the following command to uninstall openldap-clients.

```
# dnf remove openldap-clients
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

3 Network Configuration

This section provides guidance on for securing the network configuration of the system through kernel parameters, access list control, and firewall settings.

3.1 Network Parameters (Host Only)

The following network parameters are intended for use if the system is to act as a host only. A system is considered host only if the system has a single interface, or has multiple interfaces but will not be configured as a router.

Note:

- sysctl settings are defined through files in `/usr/lib/sysctl.d/`, `/run/sysctl.d/`, and `/etc/sysctl.d/`.
- Files must have the ".conf" extension.
- Vendors settings live in `/usr/lib/sysctl.d/`
- To override a whole file, create a new file with the same name in `/etc/sysctl.d/` and put new settings there.
- To override only specific settings, add a file with a lexically later name in `/etc/sysctl.d/` and put new settings there.
- The paths where sysctl preload files usually exist
 - `/run/sysctl.d/*.conf`
 - `/etc/sysctl.d/*.conf`
 - `/usr/local/lib/sysctl.d/*.conf`
 - `/usr/lib/sysctl.d/*.conf`
 - `/lib/sysctl.d/*.conf`
 - `/etc/sysctl.conf`

3.1.1 Ensure IP forwarding is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `net.ipv4.ip_forward` and `net.ipv6.conf.all.forwarding` flags are used to tell the system whether it can forward packets or not.

Rationale:

Setting the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.ip_forward  
  
net.ipv4.ip_forward = 0  
  
# grep -E -s "^\s*net\.ipv4\.ip_forward\s*=\s*1" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf  
  
No value should be returned
```

If IPv6 is enabled:

Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.forwarding  
  
net.ipv6.conf.all.forwarding = 0  
  
# grep -E -s "^\s*net\.ipv6\.conf\.all\.forwarding\s*=\s*1" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf  
  
No value should be returned
```

Remediation:

Run the following commands to restore the default parameters and set the active kernel parameters:

```
# grep -Els "^s*net\.ipv4\.ip_forward\s*=\s*1" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while  
read filename; do sed -ri "s/^s*(net\.ipv4\.ip_forward\s*)\s*=\s*(\S+)(.*$)/#  
*REMOVED* \1/" $filename; done; sysctl -w net.ipv4.ip_forward=0; sysctl -w  
net.ipv4.route.flush=1  
  
# grep -Els "^s*net\.ipv6\.conf\.all\.forwarding\s*=\s*1" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while  
read filename; do sed -ri  
"s/^s*(net\.ipv6\.conf\.all\.forwarding\s*)\s*=\s*(\S+)(.*$)/# *REMOVED* \1/"  
$filename; done; sysctl -w net.ipv6.conf.all.forwarding=0; sysctl -w  
net.ipv6.route.flush=1
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230540

Rule ID: SV-230540r627750_rule

STIG ID: RHEL-08-040260

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.1.2 Ensure packet redirect sending is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects.

Rationale:

An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.send_redirects  
  
net.ipv4.conf.all.send_redirects = 0  
  
# sysctl net.ipv4.conf.default.send_redirects  
  
net.ipv4.conf.default.send_redirects = 0  
  
# grep "net\.ipv4\.conf\.all\.send_redirects" /etc/sysctl.conf  
/etc/sysctl.d/*  
  
net.ipv4.conf.all.send_redirects = 0  
  
# grep "net\.ipv4\.conf\.default\.send_redirects" /etc/sysctl.conf  
/etc/sysctl.d/*  
  
net.ipv4.conf.default.send_redirects= 0
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.all.send_redirects = 0  
net.ipv4.conf.default.send_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.send_redirects=0  
# sysctl -w net.ipv4.conf.default.send_redirects=0  
# sysctl -w net.ipv4.route.flush=1
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230536

Rule ID: SV-230536r744037_rule

STIG ID: RHEL-08-040220

Severity: CAT II

Vul ID: V-230543

Rule ID: SV-230543r744047_rule

STIG ID: RHEL-08-040270

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.1.3 Ensure the system does not accept router advertisements on IPv6 interfaces, unless the system is a router (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not accept router advertisements on all IPv6 interfaces.

Rationale:

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

An illicit router advertisement message could result in a man-in-the-middle attack.

Audit:

Verify the operating system does not accept router advertisements on all IPv6 interfaces, unless the system is a router.

Note: If IPv6 is disabled on the system, this requirement is not applicable.

Check to see if router advertisements are not accepted by using the following command:

```
# sysctl net.ipv6.conf.all.accept_ra  
net.ipv6.conf.all.accept_ra = 0
```

If the "accept_ra" value is not "0" and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the operating system to not accept router advertisements on all IPv6 interfaces unless the system is a router with the following commands:

```
# sysctl -w net.ipv6.conf.all.accept_ra=0
```

If "0" is not the system's default value then add or update the following lines in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.all.accept_ra=0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230541

Rule ID: SV-230541r627750_rule

STIG ID: RHEL-08-040261

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.1.4 Ensure the system does not accept router advertisements on IPv6 interfaces by default, unless the system is a router (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not accept router advertisements on all IPv6 interfaces by default.

Rationale:

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

An illicit router advertisement message could result in a man-in-the-middle attack.

Audit:

Verify the operating system does not accept router advertisements on all IPv6 interfaces by default, unless the system is a router.

Note: If IPv6 is disabled on the system, this requirement is not applicable.

Check to see if router advertisements are not accepted by default by using the following command:

```
# sysctl net.ipv6.conf.default.accept_ra  
net.ipv6.conf.default.accept_ra = 0
```

If the "accept_ra" value is not "0" and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the operating system to not accept router advertisements on all IPv6 interfaces by default unless the system is a router with the following commands:

```
# sysctl -w net.ipv6.conf.default.accept_ra=0
```

If "0" is not the system's default value then add or update the following lines in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.default.accept_ra=0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230542

Rule ID: SV-230542r627750_rule

STIG ID: RHEL-08-040262

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2 Network Parameters (Host and Router)

The following network parameters are intended for use on both host only and router systems. A system acts as a router if it has at least two interfaces and is configured to perform routing functions.

Note:

- sysctl settings are defined through files in `/usr/lib/sysctl.d/`, `/run/sysctl.d/`, and `/etc/sysctl.d/`.
- Files must have the ".conf" extension.
- Vendors settings live in `/usr/lib/sysctl.d/`
- To override a whole file, create a new file with the same name in `/etc/sysctl.d/` and put new settings there.
- To override only specific settings, add a file with a lexically later name in `/etc/sysctl.d/` and put new settings there.
- The paths where sysctl preload files usually exist
 - `/run/sysctl.d/*.conf`
 - `/etc/sysctl.d/*.conf`
 - `/usr/local/lib/sysctl.d/*.conf`
 - `/usr/lib/sysctl.d/*.conf`
 - `/lib/sysctl.d/*.conf`
 - `/etc/sysctl.conf`

3.2.1 Ensure source routed packets are not accepted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

Rationale:

Setting `net.ipv4.conf.all.accept_source_route`,
`net.ipv4.conf.default.accept_source_route`,
`net.ipv6.conf.all.accept_source_route` and
`net.ipv6.conf.default.accept_source_route` to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.accept_source_route  
  
net.ipv4.conf.all.accept_source_route = 0  
  
# sysctl net.ipv4.conf.default.accept_source_route  
  
net.ipv4.conf.default.accept_source_route = 0  
  
# grep "net\.ipv4\.conf\.all\.accept_source_route" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf  
  
net.ipv4.conf.all.accept_source_route= 0  
  
# grep "net\.ipv4\.conf\.default\.accept_source_route" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf  
  
net.ipv4.conf.default.accept_source_route= 0
```

If IPv6 is enabled:

Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.accept_source_route  
  
net.ipv6.conf.all.accept_source_route = 0  
  
# sysctl net.ipv6.conf.default.accept_source_route  
  
net.ipv6.conf.default.accept_source_route = 0  
  
# grep "net\.ipv6\.conf\.all\.accept_source_route" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf  
  
net.ipv6.conf.all.accept_source_route= 0  
  
# grep "net\.ipv6\.conf\.default\.accept_source_route" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf  
  
net.ipv6.conf.default.accept_source_route= 0
```

Remediation:

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:

```
net.ipv4.conf.all.accept_source_route = 0  
net.ipv4.conf.default.accept_source_route = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.accept_source_route=0  
# sysctl -w net.ipv4.conf.default.accept_source_route=0  
# sysctl -w net.ipv4.route.flush=1
```

If IPv6 is not disabled:

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:

```
net.ipv6.conf.all.accept_source_route = 0  
net.ipv6.conf.default.accept_source_route = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv6.conf.all.accept_source_route=0  
# sysctl -w net.ipv6.conf.default.accept_source_route=0  
# sysctl -w net.ipv6.route.flush=1
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.2 Ensure ICMP redirects are not accepted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting

`net.ipv4.conf.all.accept_redirects` and `net.ipv6.conf.all.accept_redirects` to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Rationale:

Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.accept_redirects  
  
net.ipv4.conf.all.accept_redirects = 0  
  
# sysctl net.ipv4.conf.default.accept_redirects  
  
net.ipv4.conf.default.accept_redirects = 0  
  
# grep "net\.ipv4\.conf\.all\.accept_redirects" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf  
  
net.ipv4.conf.all.accept_redirects= 0  
  
# grep "net\.ipv4\.conf\.default\.accept_redirects" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf  
  
net.ipv4.conf.default.accept_redirects= 0
```

If IPv6 is not disabled:

Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.accept_redirects  
  
net.ipv6.conf.all.accept_redirects = 0  
  
# sysctl net.ipv6.conf.default.accept_redirects  
  
net.ipv6.conf.default.accept_redirects = 0  
  
# grep "net\.ipv6\.conf\.all\.accept_redirects" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf  
  
net.ipv6.conf.all.accept_redirects= 0  
  
# grep "net\.ipv6\.conf\.default\.accept_redirects" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf  
  
net.ipv6.conf.default.accept_redirects= 0
```

Remediation:

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:

```
net.ipv4.conf.all.accept_redirects = 0  
net.ipv4.conf.default.accept_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.accept_redirects=0  
# sysctl -w net.ipv4.conf.default.accept_redirects=0  
# sysctl -w net.ipv4.route.flush=1
```

If IPv6 is not disabled

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:

```
net.ipv6.conf.all.accept_redirects = 0  
net.ipv6.conf.default.accept_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv6.conf.all.accept_redirects=0  
# sysctl -w net.ipv6.conf.default.accept_redirects=0  
# sysctl -w net.ipv6.route.flush=1
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.3 Ensure secure ICMP redirects are not accepted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure.

Rationale:

It is still possible for even known gateways to be compromised. Setting `net.ipv4.conf.all.secure_redirects` to 0 protects the system from routing table updates by possibly compromised known gateways.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.secure_redirects  
  
net.ipv4.conf.all.secure_redirects = 0  
  
# sysctl net.ipv4.conf.default.secure_redirects  
  
net.ipv4.conf.default.secure_redirects = 0  
  
# grep "net\.ipv4\.conf\.all\.secure_redirects" /etc/sysctl.conf  
/etc/sysctl.d/*  
  
net.ipv4.conf.all.secure_redirects= 0  
  
# grep "net\.ipv4\.conf\.default\.secure_redirects" /etc/sysctl.conf  
/etc/sysctl.d/*  
  
net.ipv4.conf.default.secure_redirects= 0
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.all.secure_redirects = 0  
net.ipv4.conf.default.secure_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.secure_redirects=0  
# sysctl -w net.ipv4.conf.default.secure_redirects=0  
# sysctl -w net.ipv4.route.flush=1
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.4 Ensure suspicious packets are logged (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

When enabled, this feature logs packets with un-routable source addresses to the kernel log.

Rationale:

Enabling this feature and logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.log_martians  
  
net.ipv4.conf.all.log_martians = 1  
  
# sysctl net.ipv4.conf.default.log_martians  
  
net.ipv4.conf.default.log_martians = 1  
  
# grep "net\.ipv4\.conf\.all\.log_martians" /etc/sysctl.conf /etc/sysctl.d/*  
  
net.ipv4.conf.all.log_martians = 1  
  
# grep "net\.ipv4\.conf\.default\.log_martians" /etc/sysctl.conf  
/etc/sysctl.d/*  
  
net.ipv4.conf.default.log_martians = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.all.log_martians = 1  
net.ipv4.conf.default.log_martians = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.log_martians=1  
# sysctl -w net.ipv4.conf.default.log_martians=1  
# sysctl -w net.ipv4.route.flush=1
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.</p>		●	●
v7	<p>6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p>6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

3.2.5 Ensure broadcast ICMP requests are ignored (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

Setting `net.ipv4.icmp_echo_ignore_broadcasts` to 1 will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses.

Rationale:

Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.icmp_echo_ignore_broadcasts  
net.ipv4.icmp_echo_ignore_broadcasts = 1  
  
# grep -E -s "^\\s*net\\.ipv4\\.icmp_echo_ignore_broadcasts\\s*=\\s*0"  
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf  
/run/sysctl.d/*.conf  
  
Nothing should be returned
```

Remediation:

Run the following command to restore the default parameters and set the active kernel parameters:

```
# grep -Els "^\\s*net\\.ipv4\\.icmp_echo_ignore_broadcasts\\s*=\\s*0"  
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf  
/run/sysctl.d/*.conf | while read filename; do sed -ri  
"s/^\\s*(net\\.ipv4\\.icmp_echo_ignore_broadcasts\\s*) (=) (\\s*\\S+\\b).*$/#  
*REMOVED* \\1/" $filename; done; sysctl -w net.icmp_echo_ignore_broadcasts=1;  
sysctl -w net.ipv4.route.flush=1
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230537

Rule ID: SV-230537r744039_rule

STIG ID: RHEL-08-040230

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

3.2.6 Ensure bogus ICMP responses are ignored (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Setting `icmp_ignore_bogus_error_responses` to 1 prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages.

Rationale:

Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.icmp_ignore_bogus_error_responses  
  
net.ipv4.icmp_ignore_bogus_error_responses = 1  
  
# grep -E -s "^\\s*net\\.ipv4\\.icmp_ignore_bogus_error_responses\\s*=\\s*0"  
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf  
/run/sysctl.d/*.conf  
  
Nothing should be returned
```

Remediation:

Run the following commands to restore the default parameters and set the active kernel parameters:

```
# grep -Els "^\s*net\\.ipv4\\.icmp_ignore_bogus_error_responses\\s*=\\s*0"  
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf  
/run/sysctl.d/*.conf | while read filename; do sed -ri  
"s/^\\s*(net\\.ipv4\\.icmp_ignore_bogus_error_responses\\s*) (=) (\\s*\\S+\\b).*$/#  
*REMOVED* \\1/" $filename; done; sysctl -w  
net.ipv4.icmp_ignore_bogus_error_responses=1; sysctl -w  
net.ipv4.route.flush=1
```

Default Value:

`net.ipv4.icmp_ignore_bogus_error_responses = 1`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.7 Ensure Reverse Path Filtering is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

Setting `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` to 1 forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the packet is dropped (and logged if `log_martians` is set).

Rationale:

Setting these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.rp_filter
net.ipv4.conf.all.rp_filter = 1

# sysctl net.ipv4.conf.default.rp_filter
net.ipv4.conf.default.rp_filter = 1

# grep -E -s "^\s*net\.ipv4\.conf\.all\.rp_filter\s*=\s*0" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf
Nothing should be returned

# grep -E -s "^\s*net\.ipv4\.conf\.default\.rp_filter\s*=\s*1"
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf

net.ipv4.conf.default.rp_filter = 1
```

Remediation:

Run the following command to restore the default `net.ipv4.conf.all.rp_filter = 1` parameter and set the active kernel parameter:

```
# grep -Els "^\\s*net\\.ipv4\\.conf\\.all\\.rp_filter\\s*=\\s*0" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while  
read filename; do sed -ri  
"s/^\\s*(net\\.ipv4\\.net.ipv4.conf\\.all\\.rp_filter\\s*) (=) (\\s*\\S+\\b).*$/#  
*REMOVED* \\1/" $filename; done; sysctl -w net.ipv4.conf.all.rp_filter=1;  
sysctl -w net.ipv4.route.flush=1
```

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.default.rp_filter=1
```

Run the following commands to set the active kernel parameter:

```
# sysctl -w net.ipv4.conf.default.rp_filter=1  
# sysctl -w net.ipv4.route.flush=1
```

Default Value:

`net.ipv4.conf.all.rp_filter = 1`
`net.ipv4.conf.default.rp_filter = 0`

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230549

Rule ID: SV-230549r627750_rule

STIG ID: RHEL-08-040285

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.8 Ensure TCP SYN Cookies is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

When `tcp_syncookies` is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

Rationale:

Attackers use SYN flood attacks to perform a denial of service attack on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.tcp_syncookies  
  
net.ipv4.tcp_syncookies = 1  
  
# grep -E -r "^s*net\.ipv4\.tcp_syncookies\s*=\s*[02]" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf
```

Nothing should be returned

Remediation:

Run the following command to restore the default parameter and set the active kernel parameters:

```
# grep -Els "^s*net\.ipv4\.tcp_syncookies\s*=\s*[02]*" /etc/sysctl.conf  
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while  
read filename; do sed -ri  
"s/^s*(net\.ipv4\.tcp_syncookies\s*)\s*=\s*(\S+)\b.*$/# *REMOVED* \1/"  
$filename; done; sysctl -w net.ipv4.tcp_syncookies=1; sysctl -w  
net.ipv4.route.flush=1
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.9 Ensure IPv6 router advertisements are not accepted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This setting disables the system's ability to accept IPv6 router advertisements.

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Audit:

If IPv6 is enabled:

Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.accept_ra
net.ipv6.conf.all.accept_ra = 0

# sysctl net.ipv6.conf.default.accept_ra
net.ipv6.conf.default.accept_ra = 0

# grep "net\.ipv6\.conf\.all\.accept_ra" /etc/sysctl.conf /etc/sysctl.d/*
net.ipv6.conf.all.accept_ra = 0

# grep "net\.ipv6\.conf\.default\.accept_ra" /etc/sysctl.conf /etc/sysctl.d/*
net.ipv6.conf.default.accept_ra = 0
```

Remediation:

If IPv6 is enabled:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv6.conf.all.accept_ra = 0  
net.ipv6.conf.default.accept_ra = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv6.conf.all.accept_ra=0  
# sysctl -w net.ipv6.conf.default.accept_ra=0  
# sysctl -w net.ipv6.route.flush=1
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.10 Ensure the operating system does not accept IPv6 ICMP redirect messages (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent IPv6 Internet Control Message Protocol (ICMP) redirect messages from being accepted.

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Audit:

Verify the operating system does not accept IPv6 ICMP redirect messages.

Note: If IPv6 is disabled on the system, this requirement is Not Applicable.

Check the value of the default "accept_redirects" variables with the following command:

```
# sysctl net.ipv6.conf.default.accept_redirects  
net.ipv6.conf.default.accept_redirects = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to prevent IPv6 ICMP redirect messages from being accepted with the following command:

```
# sysctl -w net.ipv6.conf.default.accept_redirects=0
```

If "0" is not the system's default value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.default.accept_redirects=0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230535

Rule ID: SV-230535r744035_rule

STIG ID: RHEL-08-040210

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.11 Ensure the operating system does not accept IPv6 source-routed packets (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not forward IPv6 source-routed packets.

Rationale:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when forwarding is enabled and the system is functioning as a router.

Audit:

Verify the operating system does not accept IPv6 source-routed packets.

Note: If IPv6 is disabled on the system, this requirement is Not Applicable.

Check the value of the accept source route variable with the following command:

```
# sysctl net.ipv6.conf.all.accept_source_route  
net.ipv6.conf.all.accept_source_route = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to not forward IPv6 source-routed packets with the following command:

```
# sysctl -w net.ipv6.conf.all.accept_source_route=0
```

If "0" is not the system's all value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.all.accept_source_route=0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230538

Rule ID: SV-230538r744042_rule

STIG ID: RHEL-08-040240

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.12 Ensure the operating system does not accept IPv6 source-routed packets by default (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not forward IPv6 source-routed packets by default.

Rationale:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when forwarding is enabled and the system is functioning as a router.

Audit:

Verify the operating system does not accept IPv6 source-routed packets by default.

Note: If IPv6 is disabled on the system, this requirement is Not Applicable.

Check the value of the accept source route variable with the following command:

```
# sysctl net.ipv6.conf.default.accept_source_route  
net.ipv6.conf.default.accept_source_route = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to not forward IPv6 source-routed packets by default with the following command:

```
# sysctl -w net.ipv6.conf.default.accept_source_route=0
```

If "0" is not the system's default value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.default.accept_source_route=0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230539

Rule ID: SV-230539r744045_rule

STIG ID: RHEL-08-040250

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.13 Ensure the operating system ignores IPv6 ICMP redirect messages (Automated)

Profile Applicability:

- STIG

Description:

The operating system must ignore IPv6 Internet Control Message Protocol (ICMP) redirect messages.

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Audit:

Verify the operating system ignores IPv6 ICMP redirect messages.

Note: If IPv6 is disabled on the system, this requirement is Not Applicable.

Check the value of the "accept_redirects" variables with the following command:

```
# sysctl net.ipv6.conf.all.accept_redirects  
net.ipv6.conf.all.accept_redirects = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to ignore IPv6 ICMP redirect messages with the following command:

```
# sysctl -w net.ipv6.conf.all.accept_redirects=0
```

If "0" is not the system's default value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.all.accept_redirects = 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230544

Rule ID: SV-230544r744050_rule

STIG ID: RHEL-08-040280

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.14 Ensure network interfaces are not in promiscuous mode (Automated)

Profile Applicability:

- STIG

Description:

Network interfaces must not be in promiscuous mode.

Rationale:

Network interfaces in promiscuous mode allow for the capture of all network traffic visible to the system. If unauthorized individuals can access these applications, it may allow them to collect information such as logon IDs, passwords, and key exchanges between systems. If the system is being used to perform a network troubleshooting function, the use of these tools must be documented with the Information System Security Officer (ISSO) and restricted to only authorized personnel.

Audit:

Verify network interfaces are not in promiscuous mode unless approved by the ISSO and documented.

Check for the status with the following command:

```
# ip link | grep -i promisc
```

If network interfaces are found on the system in promiscuous mode and their use has not been approved by the ISSO and documented, this is a finding.

Remediation:

Configure network interfaces to turn off promiscuous mode unless approved by the ISSO and documented.

Set the promiscuous mode of an interface to off with the following command:

```
# ip link set dev <devicename> multicast off promisc off
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230554

Rule ID: SV-230554r627750_rule

STIG ID: RHEL-08-040330

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.15 Ensure the operating system does not accept IPv4 ICMP redirect messages (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent IPv4 Internet Control Message Protocol (ICMP) redirect messages from being accepted.

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Audit:

Verify the operating system will not accept IPv4 ICMP redirect messages.

Note: If IPv4 is disabled on the system, this requirement is Not Applicable.

Check the value of the default "accept_redirects" variables with the following command:

```
# sysctl net.ipv4.conf.default.accept_redirects  
net.ipv4.conf.default.accept_redirects = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to prevent IPv4 ICMP redirect messages from being accepted with the following command:

```
# sysctl -w net.ipv4.conf.default.accept_redirects=0
```

If "0" is not the system's default value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv4.conf.default.accept_redirects=0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244550

Rule ID: SV-244550r743899_rule

STIG ID: RHEL-08-040209

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.16 Ensure the operating system does not accept IPv4 source-routed packet (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not forward IPv4 source-routed packets.

Rationale:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when forwarding is enabled and the system is functioning as a router.

Audit:

Verify the operating system does not accept IPv4 source-routed packets.

Note: If IPv4 is disabled on the system, this requirement is Not Applicable.

Check the value of the accept source route variable with the following command:

```
# sysctl net.ipv4.conf.all.accept_source_route  
net.ipv4.conf.all.accept_source_route = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to not forward IPv4 source-routed packets with the following command:

```
# sysctl -w net.ipv4.conf.all.accept_source_route=0
```

If "0" is not the system's all value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv4.conf.all.accept_source_route=0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244551

Rule ID: SV-244551r743902_rule

STIG ID: RHEL-08-040239

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.17 Ensure the operating system does not accept IPv4 source-routed packets by default (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not forward IPv4 source-routed packets by default.

Rationale:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when forwarding is enabled and the system is functioning as a router.

Audit:

Verify the operating system does not accept IPv4 source-routed packets by default.

Note: If IPv4 is disabled on the system, this requirement is Not Applicable.

Check the value of the accept source route variable with the following command:

```
# sysctl net.ipv4.conf.default.accept_source_route  
net.ipv4.conf.default.accept_source_route = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to not forward IPv4 source-routed packets by default with the following command:

```
# sysctl -w net.ipv4.conf.default.accept_source_route=0
```

If "0" is not the system's default value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv4.conf.default.accept_source_route=0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244552

Rule ID: SV-244552r743905_rule

STIG ID: RHEL-08-040249

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.18 Ensure the operating system ignores IPv4 ICMP redirect messages (Automated)

Profile Applicability:

- STIG

Description:

The operating system must ignore IPv4 Internet Control Message Protocol (ICMP) redirect messages.

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Audit:

Verify the operating system ignores IPv4 ICMP redirect messages.

Note: If IPv4 is disabled on the system, this requirement is Not Applicable.

Check the value of the "accept_redirects" variables with the following command:

```
# sysctl net.ipv4.conf.all.accept_redirects  
net.ipv4.conf.all.accept_redirects = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to ignore IPv4 ICMP redirect messages with the following command:

```
# sysctl -w net.ipv4.conf.all.accept_redirects=0
```

If "0" is not the system's default value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv4.conf.all.accept_redirects = 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244553

Rule ID: SV-244553r743908_rule

STIG ID: RHEL-08-040279

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.3 Uncommon Network Protocols

The Linux kernel modules support several network protocols that are not commonly used. If these protocols are not needed, it is recommended that they be disabled in the kernel.

Note: This should not be considered a comprehensive list of uncommon network protocols, you may wish to consider additions to those listed here for your environment.

3.3.1 Ensure DCCP is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery.

Rationale:

If the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v dccp
install /bin/true

# lsmod | grep dccp
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vim /etc/modprobe.d/dccp.conf`
and add the following line:

```
install dccp /bin/true
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.3.2 Ensure SCTP is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

Description:

The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP.

Rationale:

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v sctp
install /bin/true

# lsmod | grep sctp
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vim /etc/modprobe.d/sctp.conf`
and add the following line:

```
install sctp /bin/true
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230496

Rule ID: SV-230496r744017_rule

STIG ID: RHEL-08-040023

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.3.3 Ensure RDS is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The Reliable Datagram Sockets (RDS) protocol is a transport layer protocol designed to provide low-latency, high-bandwidth communications between cluster nodes. It was developed by the Oracle Corporation.

Rationale:

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v rds
install /bin/true

# lsmod | grep rds
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vim /etc/modprobe.d/rds.conf`
and add the following line:

```
install rds /bin/true
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.3.4 Ensure TIPC is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

Description:

The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communication between cluster nodes.

Rationale:

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v tipc
install /bin/true

# lsmod | grep tipc
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vim /etc/modprobe.d/tipc.conf`
and add the following line:

```
install tipc /bin/true
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230497

Rule ID: SV-230497r627750_rule

STIG ID: RHEL-08-040024

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.3.5 Ensure ATM is disabled (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable the asynchronous transfer mode (ATM) protocol.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Failing to disconnect unused protocols can result in a system compromise.

The Asynchronous Transfer Mode (ATM) is a protocol operating on network, data link, and physical layers, based on virtual circuits and virtual paths. Disabling ATM protects the system against exploitation of any flaws in its implementation.

Audit:

Verify the operating system disables the ability to load the ATM protocol kernel module.

```
# grep -ri ATM /etc/modprobe.d/* | grep -i "/bin/true"  
install ATM /bin/true
```

If the command does not return any output, or the line is commented out, and use of the ATM protocol is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify the operating system disables the ability to use the ATM protocol.
Check to see if the ATM protocol is disabled with the following command:

```
# grep -ri ATM /etc/modprobe.d/* | grep -i "blacklist"  
blacklist ATM
```

If the command does not return any output or the output is not "blacklist atm", and use of the ATM protocol is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the operating system to disable the ability to use the ATM protocol kernel module.

Add or update the following lines in the file "/etc/modprobe.d/blacklist.conf":

```
install ATM /bin/true  
blacklist ATM
```

Reboot the system for the settings to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230494

Rule ID: SV-230494r627750_rule

STIG ID: RHEL-08-040021

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.3.6 Ensure CAN is disabled (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable the controller area network (CAN) protocol.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Failing to disconnect unused protocols can result in a system compromise.

The Controller Area Network (CAN) is a serial communications protocol, which was initially developed for automotive and is now also used in marine, industrial, and medical applications. Disabling CAN protects the system against exploitation of any flaws in its implementation.

Audit:

Verify the operating system disables the ability to load the CAN protocol kernel module.

```
# grep -ri CAN /etc/modprobe.d/* | grep -i "/bin/true"  
install CAN /bin/true
```

If the command does not return any output, or the line is commented out, and use of the CAN protocol is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify the operating system disables the ability to use the CAN protocol.
Check to see if the CAN protocol is disabled with the following command:

```
# grep -ri CAN /etc/modprobe.d/* | grep -i "blacklist"  
blacklist CAN
```

If the command does not return any output or the output is not "blacklist CAN", and use of the CAN protocol is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the operating system to disable the ability to use the CAN protocol kernel module.

Add or update the following lines in the file "/etc/modprobe.d/blacklist.conf":

```
install CAN /bin/true  
blacklist CAN
```

Reboot the system for the settings to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230495

Rule ID: SV-230495r627750_rule

STIG ID: RHEL-08-040022

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.4 Firewall Configuration

A firewall is a set of rules. When a data packet moves into or out of a protected network space, its contents (in particular, information about its origin, target, and the protocol it plans to use) are tested against the firewall rules to see if it should be allowed through. To provide a Host Based Firewall, the Linux kernel includes support for:

- Netfilter - A set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack. Includes the ip_tables, ip6_tables, arp_tables, and ebtables kernel modules. These modules are some of the significant parts of the Netfilter hook system.
- nftables - A subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames. nftables is supposed to replace certain parts of Netfilter, while keeping and reusing most of it. nftables utilizes the building blocks of the Netfilter infrastructure, such as the existing hooks into the networking stack, connection tracking system, userspace queueing component, and logging subsystem. **Is available in Linux kernels 3.13 and newer.**

In order to configure firewall rules for Netfilter or nftables, a firewall utility needs to be installed. Guidance has been included for the following firewall utilities:

- FirewallD - Provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the iptables backend. Starting in v0.6.0, FirewallD added support for acting as a front-end for the Linux kernel's netfilter framework via the nftables userspace utility, acting as an alternative to the nft command line program. firewalld supports both IPv4 and IPv6 networks and can administer separate firewall zones with varying degrees of trust as defined in zone profiles.
- nftables - Includes the nft utility for configuration of the nftables subsystem of the Linux kernel
- iptables - Includes the iptables, ip6tables, arptables and ebtables utilities for configuration Netfilter and the ip_tables, ip6_tables, arp_tables, and ebtables kernel modules.

Note:

- *Only one method should be used to configure a firewall on the system. Use of more than one method could produce unexpected results.*
- *This section is intended only to ensure the resulting firewall rules are in place, not how they are configured.*

3.4.1 Ensure Firewall software is installed

In order to configure Firewall protection for your system, a Firewall software package needs to be installed.

3.4.1.1 Ensure a Firewall package is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A Firewall package should be selected. Most firewall configuration utilities operate as a front end to nftables or iptables.

Rationale:

A Firewall package is required for firewall management and configuration.

Audit:

Run **one** of the following commands to verify the Firewall package is installed:

For firewalld:

```
# rpm -q firewalld  
firewalld-<version>
```

For nftables:

```
# rpm -q nftables  
nftables-<version>
```

For iptables:

```
# rpm -q iptables iptables-services  
iptables-<version>  
iptables-services-<version>
```

Remediation:

Run **one** of the following commands to install a Firewall package.

For firewalld:

```
# dnf install firewalld
```

For nftables:

```
# dnf install nftables
```

For iptables:

```
# dnf install iptables iptables-services
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.2 Configure firewalld

If nftables or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

firewalld (Dynamic Firewall Manager) provides a dynamically managed firewall with support for network/firewall “zones” to assign a level of trust to a network and its associated connections, interfaces or sources. It has support for IPv4, IPv6, Ethernet bridges and also for IPSet firewall settings. There is a separation of the runtime and permanent configuration options. It also provides an interface for services or applications to add iptables, ip6tables and ebtables rules directly. This interface can also be used by advanced users.

In the v0.6.0 release, firewalld gained support for using nftables as a firewall back-end.

Note: Configuration of a live system's firewall directly over a remote connection will often result in being locked out.

3.4.2.1 Ensure firewalld service is enabled and running (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

Ensure that the firewalld service is enabled to protect your system

Rationale:

firewalld (Dynamic Firewall Manager) tool provides a dynamically managed firewall. The tool enables network/firewall zones to define the trust level of network connections and/or interfaces. It has support both for IPv4 and IPv6 firewall settings. Also, it supports Ethernet bridges and allow you to separate between runtime and permanent configuration options. Finally, it supports an interface for services or applications to add firewall rules directly

Impact:

Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following command to verify that firewalld is enabled:

```
# systemctl is-enabled firewalld  
enabled
```

Run the following command to verify that firewalld is running

```
# firewall-cmd --state  
running
```

Remediation:

Run the following command to enable and start firewalld

```
# systemctl --now enable firewalld
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244544

Rule ID: SV-244544r743881_rule

STIG ID: RHEL-08-040101

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.2.2 Ensure iptables service is not enabled with firewalld (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

IPtables is an application that allows a system administrator to configure the IPv4 and IPv6 tables, chains and rules provided by the Linux kernel firewall.
IPtables is installed as a dependency with firewalld.

Rationale:

Running firewalld and IPtables concurrently may lead to conflict, therefore IPtables should be stopped and masked when using firewalld.

Audit:

Run the following command to verify that iptables is not running:

```
# systemctl status iptables
```

Output should include:

```
Loaded: disabled (/dev/null; bad)
Active: inactive (dead)
```

Run the following command to verify that iptables is not enabled:

```
# systemctl is-enabled iptables
```

Output should not read `enabled`

Remediation:

Run the following command to stop and mask iptables

```
systemctl --now mask iptables
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●

3.4.2.3 Ensure nftables is not enabled with firewalld (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables.
nftables are installed as a dependency with firewalld.

Rationale:

Running firewalld and nftables concurrently may lead to conflict, therefore nftables should be stopped and masked when using firewalld.

Audit:

Run the following command to verify that nftables is not enabled:

```
# systemctl is-enabled nftables  
(disabled|masked)
```

Run the following command to verify that nftables is not running:

```
# systemctl status nftables
```

Output should include:

```
Loaded: masked (/dev/null; bad)  
Active: inactive (dead)
```

Remediation:

Run the following command to mask and stop nftables

```
systemctl --now mask nftables
```

Additional Information:

firewalld is dependent on nftables. nftables should be stopped and disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●

3.4.2.4 Ensure firewalld default zone is set (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A firewall zone defines the trust level for a connection, interface or source address binding. This is a one to many relation, which means that a connection, interface or source can only be part of one zone, but a zone can be used for many network connections, interfaces and sources.

The default zone is the zone that is used for everything that is not explicitly bound/assigned to another zone.

That means that if there is no zone assigned to a connection, interface or source, only the default zone is used. The default zone is not always listed as being used for an interface or source as it will be used for it either way. This depends on the manager of the interfaces. Connections handled by NetworkManager are listed as NetworkManager requests to add the zone binding for the interface used by the connection. Also interfaces under control of the network service are listed also because the service requests it.

Rationale:

Because the default zone is the zone that is used for everything that is not explicitly bound/assigned to another zone, it is important for the default zone to set

Audit:

Run the following command and verify that the default zone adheres to company policy:

```
# firewall-cmd --get-default-zone
```

Remediation:

Run the following command to set the default zone:

```
# firewall-cmd --set-default-zone=<NAME_OF_ZONE>
```

Example:

```
# firewall-cmd --set-default-zone=public
```

References:

1. <https://firewalld.org/documentation>
2. <https://firewalld.org/documentation/man-pages/firewalld.zone>

Additional Information:

A firewalld zone configuration file contains the information for a zone. These are the zone description, services, ports, protocols, icmp-blocks, masquerade, forward-ports and rich language rules in an XML file format. The file name has to be `zone_name.xml` where length of `zone_name` is currently limited to 17 chars.

NetworkManager binds interfaces to zones automatically

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.2.5 Ensure network interfaces are assigned to appropriate zone (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

firewall zones define the trust level of network connections or interfaces.

Rationale:

A network interface not assigned to the appropriate zone can allow unexpected or undesired network traffic to be accepted on the interface

Impact:

Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following command, and verify that the interface(s) follow site policy for zone assignment

```
# nmcli -t connection show | awk -F: '{if($4){print $4}}' | while read INT; do firewall-cmd --get-active-zones | grep -B1 $INT; done
```

Remediation:

Run the following command to assign an interface to the appropriate zone.

```
# firewall-cmd --zone=<Zone NAME> --change-interface=<INTERFACE NAME>
```

Example:

```
# firewall-cmd --zone=customzone --change-interface=eth0
```

Default Value:

If the zone is not set in the configuration file, the interfaces will be assigned to the default zone defined in the firewalld configuration

References:

1. <https://firewalld.org/documentation/zone/connections-interfaces-and-sources.html>

Additional Information:

The firewall in the Linux kernel is not able to handle network connections with the name shown by NetworkManager, it can only handle the network interfaces used by the connection. Because of this NetworkManager tells firewalld to assign the network interface that is used for this connection to the zone defined in the configuration of that connection. This assignment happens before the interface is used. The configuration of the connection can either be the NetworkManager configuration or also an ifcfg for example. If the zone is not set in the configuration file, the interfaces will be assigned to the default zone defined in the firewalld configuration. If a connection has more than one interface, all of them will be supplied to firewalld. Also changes in the names of interfaces will be handled by NetworkManager and supplied to firewalld.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.2.6 Ensure firewalld drops unnecessary services and ports (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Services and ports can be accepted or explicitly rejected or dropped by a zone. For every zone, you can set a default behavior that handles incoming traffic that is not further specified. Such behavior is defined by setting the target of the zone. There are three options - default, ACCEPT, REJECT, and DROP.

By setting the target to ACCEPT, you accept all incoming packets except those disabled by a specific rule.

If you set the target to REJECT or DROP, you disable all incoming packets except those that you have allowed in specific rules. When packets are rejected, the source machine is informed about the rejection, while there is no information sent when the packets are dropped.

Rationale:

To reduce the attack surface of a system, all services and ports should be blocked unless required

Audit:

Run the following command and review output to ensure that listed services and ports follow site policy.

```
# firewall-cmd --get-active-zones | awk '!/:/ {print $1}' | while read ZN; do  
firewall-cmd --list-all --zone=$ZN; done
```

Remediation:

Run the following command to remove an unnecessary service:

```
# firewall-cmd --remove-service=<service>
```

Example:

```
# firewall-cmd --remove-service=cockpit
```

Run the following command to remove an unnecessary port:

```
# firewall-cmd --remove-port=<port-number>/<port-type>
```

Example:

```
# firewall-cmd --remove-port=25/tcp
```

Run the following command to make new settings persistent:

```
# firewall-cmd --runtime-to-permanent
```

References:

1. firewalld.service(5)
2. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/securing_networks/using-and-configuring_firewalls_securing-networks

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.2.7 Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems (Manual)

Profile Applicability:

- STIG

Description:

The firewall must employ a deny-all, allow-by-exception policy for allowing connections to other systems.

Rationale:

Failure to restrict network connectivity only to authorized systems permits inbound connections from malicious systems. It also permits outbound connections that may facilitate exfiltration of DoD data.

The operating system incorporates the "firewalld" daemon, which allows for many different configurations. One of these configurations is zones. Zones can be utilized to a deny-all, allow-by-exception approach. The default "drop" zone will drop all incoming network packets unless it is explicitly allowed by the configuration file or is related to an outgoing network connection.

Audit:

Verify "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems with the following commands:

```
# firewall-cmd --state  
running  
  
# firewall-cmd --get-active-zones  
  
[custom]  
interfaces: ens33  
  
# firewall-cmd --info-zone=[custom] | grep target  
  
target: DROP
```

If no zones are active on the operating system's interfaces or if the target is set to a different option other than "DROP", this is a finding.

Remediation:

Configure the "firewalld" daemon to employ a deny-all, allow-by-exception with the following commands:

```
# firewall-cmd --permanent --new-zone=[custom]  
# cp /usr/lib/firewalld/zones/drop.xml /etc/firewalld/zones/[custom].xml
```

This will provide a clean configuration file to work with that employs a deny-all approach. Next, add the exceptions that are required for mission functionality.

```
# firewall-cmd --set-default-zone=[custom]
```

Note: This is a runtime and permanent change.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230504

Rule ID: SV-230504r627750_rule

STIG ID: RHEL-08-040090

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.2.8 Ensure "firewalld" is installed (Automated)

Profile Applicability:

- STIG

Description:

A firewall must be installed on the operating system.

Rationale:

"Firewalld" provides an easy and effective way to block/limit remote access to the system via ports, services, and protocols.

Remote access services, such as those providing remote access to network devices and information systems, which lack automated control capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless. The operating system's functionality (e.g., RDP) must be capable of taking enforcement action if the audit reveals unauthorized activity. Automated control of remote access sessions allows organizations to ensure ongoing compliance with remote access policies by enforcing connection rules of remote access applications on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Audit:

Verify that "firewalld" is installed with the following commands:

```
# yum list installed firewalld  
firewalld.noarch 0.7.0-5.el8
```

If the "firewalld" package is not installed, ask the System Administrator if another firewall is installed. If no firewall is installed this is a finding.

Remediation:

Install "firewalld" with the following command:

```
# yum install firewalld.noarch
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230505

Rule ID: SV-230505r744020_rule

STIG ID: RHEL-08-040100

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.3 Configure nftables

If firewalld or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables. The biggest change with the successor nftables is its simplicity. With iptables, we have to configure every single rule and use the syntax which can be compared with normal commands. With nftables, the simpler syntax, much like BPF (Berkely Packet Filter) means shorter lines and less repetition.

Support for nftables should also be compiled into the kernel, together with the related nftables modules. It is available in Linux kernels >= 3.13. **Please ensure that your kernel supports nftables before choosing this option.**

This section broadly assumes starting with an empty nftables firewall ruleset (established by flushing the rules with nft flush ruleset). Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot. **Configuration of a live systems firewall directly over a remote connection will often result in being locked out.** It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

Note: Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

The following will implement the firewall rules of this section and open ICMP, IGMP, and port 22(ssh) from anywhere. Opening the ports for ICMP, IGMP, and port 22(ssh) needs to be updated in accordance with local site policy. Allow port 22(ssh) needs to be updated to only allow systems requiring ssh connectivity to connect, as per site policy.

Save the script bellow as /etc/nftables/nftables.rules

```
#!/sbin/nft -f

# This nftables.rules config should be saved as /etc/nftables/nftables.rules

# flush nftables ruleset

flush ruleset

# Load nftables ruleset

# nftables config with inet table named filter

table inet filter {

    # Base chain for input hook named input (Filters inbound network
    packets)

    chain input {

        type filter hook input priority 0; policy drop;

        # Ensure loopback traffic is configured

        iif "lo" accept

        ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop

        ip6 saddr ::1 counter packets 0 bytes 0 drop

        # Ensure established connections are configured

        ip protocol tcp ct state established accept

        ip protocol udp ct state established accept

        ip protocol icmp ct state established accept

        # Accept port 22(SSH) traffic from anywhere
```

```

        tcp dport ssh accept

        # Accept ICMP and IGMP from anywhere

        icmpv6 type { destination-unreachable, packet-too-big, time-
exceeded, parameter-problem, mld-listener-query, mld-listener-report, mld-
listener-done, nd-router-solicit, nd-router-advert, nd-neighbor-solicit, nd-
neighbor-advert, ind-neighbor-solicit, ind-neighbor-advert, mld2-listener-
report } accept

        icmp type { destination-unreachable, router-advertisement,
router-solicitation, time-exceeded, parameter-problem } accept

        ip protocol igmp accept

    }

    # Base chain for hook forward named forward (Filters forwarded
network packets)

    chain forward {

        type filter hook forward priority 0; policy drop;

    }

    # Base chain for hook output named output (Filters outbound network
packets)

    chain output {

        type filter hook output priority 0; policy drop;

        # Ensure outbound and established connections are configured

        ip protocol tcp ct state established,related,new accept

        ip protocol udp ct state established,related,new accept

        ip protocol icmp ct state established,related,new accept

    }

}

```

Run the following command to load the file into nftables

```
# nft -f /etc/nftables/nftables.rules
```

All changes in the nftables subsections are temporary

To make these changes permanent:

Run the following command to create the nftables.rules file

```
nft list ruleset > /etc/nftables/nftables.rules
```

Add the following line to /etc/sysconfig/nftables.conf

```
include "/etc/nftables/nftables.rules"
```

3.4.3.1 Ensure iptables are flushed with nftables (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a replacement for iptables, ip6tables, ebtables and arptables

Rationale:

It is possible to mix iptables and nftables. However, this increases complexity and also the chance to introduce errors. For simplicity flush out all iptables rules, and ensure it is not loaded

Audit:

Run the following commands to ensure no iptables rules exist

For iptables:

```
# iptables -L
```

No rules should be returned

For ip6tables:

```
# ip6tables -L
```

No rules should be returned

Remediation:

Run the following commands to flush iptables:

For iptables:

```
# iptables -F
```

For ip6tables

```
# ip6tables -F
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●

3.4.3.2 Ensure an nftables table exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Tables hold chains. Each table only has one address family and only applies to packets of this family. Tables can have one of five families.

Rationale:

nftables doesn't have any default tables. Without a table being build, nftables will not filter network traffic.

Impact:

Adding rules to a running nftables can cause loss of connectivity to the system

Audit:

Run the following command to verify that a nftables table exists:

```
# nft list tables
```

Return should include a list of nftables:

example:

```
table inet filter
```

Remediation:

Run the following command to create a table in nftables

```
# nft create table inet <table name>
```

Example:

```
# nft create table inet filter
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.3.3 Ensure nftables base chains exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

Rationale:

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

Impact:

if configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

Audit:

Run the following commands and verify that base chains exist for INPUT, FORWARD, and OUTPUT.

```
# nft list ruleset | grep 'hook input'  
  
type filter hook input priority 0;  
  
# nft list ruleset | grep 'hook forward'  
  
type filter hook forward priority 0;  
  
# nft list ruleset | grep 'hook output'  
  
type filter hook output priority 0;
```

Remediation:

Run the following command to create the base chains:

```
# nft create chain inet <table name> <base chain name> { type filter hook <(input|forward|output)> priority 0 \; }
```

Example:

```
# nft create chain inet filter input { type filter hook input priority 0 \; }

# nft create chain inet filter forward { type filter hook forward priority 0 \; }

# nft create chain inet filter output { type filter hook output priority 0 \; }
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.3.4 Ensure nftables loopback traffic is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network

Rationale:

Loopback traffic is generated between processes on a machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Audit:

Run the following commands to verify that the loopback interface is configured:

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'iif "lo" accept'  
iif "lo" accept  
  
# nft list ruleset | awk '/hook input/,/}/' | grep 'ip saddr'  
ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
```

If IPv6 is enabled, run the following command to verify that the IPv6 loopback interface is configured:

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'ip6 saddr'  
ip6 saddr ::1 counter packets 0 bytes 0 drop
```

Remediation:

Run the following commands to implement the loopback rules:

```
# nft add rule inet filter input iif lo accept  
# nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop
```

If IPv6 is enabled:

Run the following command to implement the IPv6 loopback rules:

```
# nft add rule inet filter input ip6 saddr ::1 counter drop
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p>19.4 Devise Organization-wide Standards for Reporting Incidents Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.</p>		●	●

3.4.3.5 Ensure nftables outbound and established connections are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound, and established connections

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Audit:

Run the following commands and verify all rules for established incoming connections match site policy: site policy:

```
# nft list ruleset | awk '/hook input/,/}/' | grep -E 'ip protocol (tcp|udp|icmp) ct state'
```

Output should be similar to:

```
ip protocol tcp ct state established accept
ip protocol udp ct state established accept
ip protocol icmp ct state established accept
```

Run the following command and verify all rules for new and established outbound connections match site policy

```
# nft list ruleset | awk '/hook output/,/}/' | grep -E 'ip protocol (tcp|udp|icmp) ct state'
```

Output should be similar to:

```
ip protocol tcp ct state established,related,new accept
ip protocol udp ct state established,related,new accept
ip protocol icmp ct state established,related,new accept
```

Remediation:

Configure nftables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# nft add rule inet filter input ip protocol tcp ct state established accept  
# nft add rule inet filter input ip protocol udp ct state established accept  
# nft add rule inet filter input ip protocol icmp ct state established accept  
  
# nft add rule inet filter output ip protocol tcp ct state  
new,related,established accept  
  
# nft add rule inet filter output ip protocol udp ct state  
new,related,established accept  
  
# nft add rule inet filter output ip protocol icmp ct state  
new,related,established accept
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.3.6 Ensure nftables default deny firewall policy (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

Rationale:

There are two policies: accept (Default) and drop. If the policy is set to accept, the firewall will accept any packet that is not configured to be denied and the packet will continue transversing the network stack.

It is easier to white list acceptable usage than to black list unacceptable usage.

Impact:

If configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

Audit:

Run the following commands and verify that base chains contain a policy of DROP.

```
# nft list ruleset | grep 'hook input'  
  
type filter hook input priority 0; policy drop;  
  
# nft list ruleset | grep 'hook forward'  
  
type filter hook forward priority 0; policy drop;  
  
# nft list ruleset | grep 'hook output'  
  
type filter hook output priority 0; policy drop;
```

Remediation:

Run the following command for the base chains with the input, forward, and output hooks to implement a default DROP policy:

```
# nft chain <table family> <table name> <chain name> { policy drop \; }
```

Example:

```
# nft chain inet filter input { policy drop \; }
# nft chain inet filter forward { policy drop \; }
# nft chain inet filter output { policy drop \; }
```

Default Value:

accept

References:

1. Manual Page nft

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.3.7 Ensure nftables service is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The nftables service allows for the loading of nftables rulesets during boot, or starting of the nftables service

Rationale:

The nftables service restores the nftables rules from the rules files referenced in the /etc/sysconfig/nftables.conf file during boot or the starting of the nftables service

Audit:

Run the following command and verify that the nftables service is enabled:

```
# systemctl is-enabled nftables  
enabled
```

Remediation:

Run the following command to enable the nftables service:

```
# systemctl --now enable nftables
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.3.8 Ensure nftables rules are permanent (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames.

The nftables service reads the `/etc/sysconfig/nftables.conf` file for a nftables file or files to include in the nftables ruleset.

A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.

Rationale:

Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot.

Audit:

Run the following commands to verify that input, forward, and output base chains are configured to be applied to a nftables ruleset on boot and follow local site policy:

Run the following command to verify the input base chain:

```
# [[ -n $(grep -E "^\s*include" /etc/sysconfig/nftables.conf) ]] && awk  
'/hook input/,/}/' $(awk '$1 ~ /^\\s*include/ { gsub("\\\"","\"",\$2);print \$2 }'  
/etc/sysconfig/nftables.conf)
```

Output should be similar to:

```
type filter hook input priority 0; policy drop;

# Ensure loopback traffic is configured
iif "lo" accept
ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
ip6 saddr ::1 counter packets 0 bytes 0 drop

# Ensure established connections are configured
ip protocol tcp ct state established accept
ip protocol udp ct state established accept
ip protocol icmp ct state established accept

# Accept port 22(SSH) traffic from anywhere
tcp dport ssh accept

# Accept ICMP and IGMP from anywhere
icmpv6 type { destination-unreachable, packet-too-big, time-exceeded,
parameter-problem, mld-listener-query, mld-listener-report, mld-listener-
done, nd-router-solicit, nd-router-advert, nd-neighbor-solicit, nd-neighbor-
advert, ind-neighbor-solicit, ind-neighbor-advert, mld2-listener-report }
accept
```

Run the following command to verify the forward base chain:

```
# [[ -n $(grep -E "^\\s*include" /etc/sysconfig/nftables.conf) ]] && awk
'hook forward/,/ /' $(awk '$1 ~ /^\\s*include/ { gsub("\\\"","\",$2);print $2 }'
/etc/sysconfig/nftables.conf)
```

Output should be similar to:

```
# Base chain for hook forward named forward (Filters forwarded network
packets)
chain forward {
    type filter hook forward priority 0; policy drop;
}
```

Run the following command to verify the output base chain:

```
# [[ -n $(grep -E "^\\s*include" /etc/sysconfig/nftables.conf) ]] && awk
'hook output/,/ /' $(awk '$1 ~ /^\\s*include/ { gsub("\\\"","\",$2);print $2 }'
/etc/sysconfig/nftables.conf)
```

Output should be similar to:

```
# Base chain for hook output named output (Filters outbound network packets)
chain output {
    type filter hook output priority 0; policy drop;
    # Ensure outbound and established connections are configured
    ip protocol tcp ct state established,related,new accept
    ip protocol tcp ct state established,related,new accept
    ip protocol udp ct state established,related,new accept
    ip protocol icmp ct state established,related,new accept
}
```

Remediation:

Edit the `/etc/sysconfig/nftables.conf` file and un-comment or add a line with `include <Absolute path to nftables rules file>` for each nftables file you want included in the nftables ruleset on boot

Example:

```
# vi /etc/sysconfig/nftables.conf
```

Add the line:

```
include "/etc/nftables/nftables.rules"
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.3.9 Ensure "nftables" is configured to allow rate limits on any connection to the system (Automated)

Profile Applicability:

- STIG

Description:

A firewall must be able to protect against or limit the effects of Denial of Service (DoS) attacks by ensuring the operating system can implement rate-limiting measures on impacted network interfaces.

Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exists to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Since version 0.6.0, "firewalld" has incorporated "nftables" as its backend support. Utilizing the limit statement in "nftables" can help to mitigate DoS attacks.

Audit:

Verify "nftables" is configured to allow rate limits on any connection to the system with the following command:

Verify "firewalld" has "nftables" set as the default backend:

```
# grep -i firewallbackend /etc/firewalld/firewalld.conf  
# FirewallBackend  
FirewallBackend=nftables
```

If the "nftables" is not set as the "firewallbackend" default, this is a finding.

Remediation:

Configure "nftables" to be the default "firewallbackend" for "firewalld" by adding or editing the following line in "etc/firewalld/firewalld.conf":

```
FirewallBackend=nftables
```

Establish rate-limiting rules based on organization-defined types of DoS attacks on impacted network interfaces.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230525

Rule ID: SV-230525r744029_rule

STIG ID: RHEL-08-040150

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.4 Configure iptables

If firewalld or nftables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

IPtables is an application that allows a system administrator to configure the IPv4 and IPv6 tables, chains and rules provided by the Linux kernel firewall. While several methods of configuration exist this section is intended only to ensure the resulting IPTables rules are in place, not how they are configured. If IPv6 is in use in your environment, similar settings should be applied to the IP6tables as well.

Note: Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

3.4.4.1 Configure IPv4 iptables

IPTables is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

Note:

- *This section broadly assumes starting with an empty IPTables firewall ruleset (established by flushing the rules with iptables -F).*
- *Configuration of a live systems firewall directly over a remote connection will often result in being locked out.*
- *It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.*

The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere. *This needs to be updated to only allow systems requiring ssh connectivity to connect as per site policy.*

```
#!/bin/bash

# Flush IPtables rules
iptables -F

# Ensure default deny firewall policy
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Ensure loopback traffic is configured
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT -s 127.0.0.0/8 -j DROP

# Ensure outbound and established connections are configured
iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

# Open inbound ssh(tcp port 22) connections
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

3.4.4.1.1 Ensure iptables loopback traffic is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Audit:

Run the following commands and verify output includes the listed rules in order (packet and byte counts may differ):

```
# iptables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out      source
destination
    0      0 ACCEPT     all   --   lo      *       0.0.0.0/0            0.0.0.0/0
    0      0 DROP       all   --   *       *       127.0.0.0/8          0.0.0.0/0

# iptables -L OUTPUT -v -n
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out      source
destination
    0      0 ACCEPT     all   --   *       lo      0.0.0.0/0            0.0.0.0/0
```

Remediation:

Run the following commands to implement the loopback rules:

```
# iptables -A INPUT -i lo -j ACCEPT
# iptables -A OUTPUT -o lo -j ACCEPT
# iptables -A INPUT -s 127.0.0.0/8 -j DROP
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.4.1.2 Ensure iptables outbound and established connections are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound, and established connections.

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Audit:

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# iptables -L -v -n
```

Remediation:

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.4.1.3 Ensure iptables firewall rules exist for all open ports (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Audit:

Run the following command to determine open ports:

```
# ss -4tuln

Netid State      Recv-Q Send-Q      Local Address:Port          Peer
Address:Port
udp    UNCONN     0      0                  *:68
*:*
udp    UNCONN     0      0                  *:123
*:*
tcp    LISTEN     0      128                *:22
*:*
```

Run the following command to determine firewall rules:

```
# iptables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out      source
destination
      0      0 ACCEPT    all   --  lo      *       0.0.0.0/0      0.0.0.0/0
      0      0 DROP      all   --  *       *       127.0.0.0/8      0.0.0.0/0
      0      0 ACCEPT    tcp   --  *       *       0.0.0.0/0      0.0.0.0/0
tcp  dpt:22 state NEW
```

Verify all open ports listening on non-localhost addresses have at least one firewall rule. The last line identified by the "tcp dpt:22 state NEW" identifies it as a firewall rule for new connections on tcp port 22.

Remediation:

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j  
ACCEPT
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.4.1.4 Ensure iptables default deny firewall policy (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Audit:

Run the following command and verify that the policy for the INPUT , OUTPUT , and FORWARD chains is DROP or REJECT :

```
# iptables -L  
  
Chain INPUT (policy DROP)  
Chain FORWARD (policy DROP)  
Chain OUTPUT (policy DROP)
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# iptables -P INPUT DROP  
# iptables -P OUTPUT DROP  
# iptables -P FORWARD DROP
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.4.1.5 Ensure iptables is enabled and active (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`iptables.service` is a utility for configuring and maintaining `iptables`.

Rationale:

`iptables.service` will load the `iptables` rules saved in the file `/etc/sysconfig/iptables` at boot, otherwise the `iptables` rules will be cleared during a re-boot of the system.

Audit:

Run the following commands to verify `iptables` is enabled:

```
# systemctl is-enabled iptables  
enabled
```

Run the following command to verify `iptables.service` is active:

```
# systemctl status iptables | grep " Active: active "  
Active: active (exited) since <day date and time>
```

Remediation:

Run the following command to enable and start `iptables`:

```
# systemctl --now enable iptables
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.4.2 Configure IPv6 ip6tables

If IPv6 is not enabled on the system, this section can be skipped.

Ip6tables is used to set up, maintain, and inspect the tables of IPv6 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

Note:

- This section broadly assumes starting with an empty ip6tables firewall ruleset (established by flushing the rules with ip6tables -F).
- Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere. This needs to be updated to only allow systems requiring ssh connectivity to connect as per site policy.

```
#!/bin/bash

# Flush ip6tables rules
ip6tables -F

# Ensure default deny firewall policy
ip6tables -P INPUT DROP
ip6tables -P OUTPUT DROP
ip6tables -P FORWARD DROP

# Ensure loopback traffic is configured
ip6tables -A INPUT -i lo -j ACCEPT
ip6tables -A OUTPUT -o lo -j ACCEPT
ip6tables -A INPUT -s ::1 -j DROP

# Ensure outbound and established connections are configured
ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

# Open inbound ssh(tcp port 22) connections
ip6tables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

3.4.4.2.1 Ensure ip6tables loopback traffic is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Audit:

If IPv6 is enabled on the system

Run the following commands and verify output includes the listed rules in order (packet and byte counts may differ):

```
# ip6tables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out      source
destination
    0      0 ACCEPT     all      lo      *       ::/0          ::/0
    0      0 DROP        all      *       *       ::1          ::/0

# ip6tables -L OUTPUT -v -n
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out      source
destination
    0      0 ACCEPT     all      *       lo      ::/0          ::/0
```

Remediation:

Run the following commands to implement the loopback rules:

```
# ip6tables -A INPUT -i lo -j ACCEPT
# ip6tables -A OUTPUT -o lo -j ACCEPT
# ip6tables -A INPUT -s ::1 -j DROP
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.4.2.2 Ensure ip6tables outbound and established connections are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound, and established IPv6 connections.

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Audit:

If IPv6 is enabled on the system

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# ip6tables -L -v -n
```

Remediation:

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.4.2.3 Ensure ip6tables firewall rules exist for all open ports (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Audit:

If IPv6 is enabled on the system

Run the following command to determine open ports:

```
# ss -6tuln

Netid State      Recv-Q Send-Q      Local Address:Port          Peer
Address:Port
udp   UNCONN      0      0              ::1:123
:::*
udp   UNCONN      0      0              :::123
:::*
tcp   LISTEN      0      128             :::22
:::*
tcp   LISTEN      0      20              ::1:25
:::*
```

Run the following command to determine firewall rules:

```
# ip6tables -L INPUT -v -n

Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out      source
destination
    0      0 ACCEPT     all      lo      *      ::/0          ::/0
    0      0 DROP       all      *      *      ::1          ::/0
    0      0 ACCEPT     tcp      *      *      ::/0          ::/0
tcp dpt:22 state NEW
```

Verify all open ports listening on non-localhost addresses have at least one firewall rule.

The last line identified by the "tcp dpt:22 state NEW" identifies it as a firewall rule for new connections on tcp port 22.

Remediation:

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# ip6tables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j
ACCEPT
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.4.2.4 Ensure ip6tables default deny firewall policy (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Audit:

If IPv6 is enabled on the system

Run the following command and verify that the policy for the INPUT, OUTPUT, and FORWARD chains is DROP or REJECT:

```
# ip6tables -L
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# ip6tables -P INPUT DROP
# ip6tables -P OUTPUT DROP
# ip6tables -P FORWARD DROP
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.4.2.5 Ensure ip6tables is enabled and active (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`ip6tables.service` is a utility for configuring and maintaining `ip6tables`.

Rationale:

`ip6tables.service` will load the iptables rules saved in the file `/etc/sysconfig/iptables` at boot, otherwise the `ip6tables` rules will be cleared during a re-boot of the system.

Audit:

If IPv6 is enabled on the system:

Run the following commands to verify `ip6tables` is enabled:

```
# systemctl is-enabled ip6tables  
enabled
```

Run the following command to verify `ip6tables.service` is active and running or exited

```
# systemctl status ip6tables | grep -E " Active: active \((running|exited)\)  
"  
  
Active: active (exited) since <day date and time>
```

Remediation:

Run the following command to enable and start `ip6tables`:

```
# systemctl --now start ip6tables
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.5 Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services (Manual)

Profile Applicability:

- STIG

Description:

The operating system must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management (PPSM) Category Assignments List (CAL) and vulnerability assessments.

Rationale:

To prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality-of-life issues.

Audit:

Inspect the firewall configuration and running services to verify it is configured to prohibit or restrict the use of functions, ports, protocols, and/or services that are unnecessary or prohibited.

Check which services are currently active with the following command:

```
# firewall-cmd --list-all-zones  
  
custom (active)  
target: DROP  
icmp-block-inversion: no  
interfaces: ens33  
sources:  
services: dhcpcv6-client dns http https ldaps rpc-bind ssh  
ports:  
masquerade: no  
forward-ports:  
icmp-blocks:  
rich rules:
```

Ask the System Administrator for the site or program Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA). Verify the services allowed by the firewall match the PPSM CLSA.

If there are additional ports, protocols, or services that are not in the PPSM CLSA, or there are ports, protocols, or services that are prohibited by the PPSM Category Assurance List (CAL), this is a finding.

Remediation:

Update the host's firewall settings and/or running services to comply with the PPSM Component Local Service Assessment (CLSA) for the site or program and the PPSM CAL.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230500

Rule ID: SV-230500r627750_rule

STIG ID: RHEL-08-040030

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.5 Ensure wireless interfaces are disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation
- STIG

Description:

Wireless networking is used when wired networks are unavailable. CentOS Linux contains a wireless tool kit to allow system administrators to configure and use wireless networks.

Rationale:

If wireless is not to be used, wireless devices can be disabled to reduce the potential attack surface.

Impact:

Many if not all laptop workstations and some desktop workstations will connect via wireless requiring these interfaces be enabled.

Audit:

Run the following command to verify no wireless interfaces are active on the system:

```
# nmcli radio all
```

Output should look like:

WIFI-HW	WIFI	WWAN-HW	WWAN
enabled	disabled	enabled	disabled

Remediation:

Run the following command to disable any wireless interfaces:

```
# nmcli radio all off
```

Disable any wireless interfaces in your network configuration.

References:

1. nmcli(1) - Linux man page

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230506

Rule ID: SV-230506r627750_rule

STIG ID: RHEL-08-040110

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	15.4 Disable Wireless Access on Devices if Not Required Disable wireless access on devices that do not have a business purpose for wireless access.			●
v7	15.5 Limit Wireless Access on Client Devices Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			●

3.6 Disable IPv6 (Manual)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Although IPv6 has many advantages over IPv4, not all organizations have IPv6 or dual stack configurations implemented.

Rationale:

If IPv6 or dual stack is not to be used, it is recommended that IPv6 be disabled to reduce the attack surface of the system.

Audit:

Run the following script to verify if IPv6 is disabled:

```
#!/bin/bash

output=""
efidir=$(find /boot/efi/EFI/* -type d -not -name 'BOOT')
gbdir=$(find /boot -maxdepth 1 -type d -name 'grub*')

[ -f "$efidir"/grubenv ] && grubfile="$efidir/grubenv" ||
grubfile="$gbdir/grubenv"

! grep "^\s*kernelopts=\"$grubfile\" | grep -vq ipv6.disable=1 &&
output="ipv6 disabled in grub config"

if grep -Eq "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b"
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && grep -Eq
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | grep -Eq
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b"; then
    [ -n "$output" ] && output="$output, and in sysctl config" || output="ipv6
disabled in sysctl config"
fi
[ -n "$output" ] && echo -e "\n\n$output\n" || echo -e "\n\nIPv6 is enabled
on the system\n"
```

Remediation:

Use **one** of the two following methods to disable IPv6 on the system:

To disable IPv6 through the GRUB2 config:

Edit `/etc/default/grub` and add `ipv6.disable=1` to the `GRUB_CMDLINE_LINUX` parameters:

```
GRUB_CMDLINE_LINUX="ipv6.disable=1"
```

Run the following command to update the `grub2` configuration:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

Or

To disable IPv6 through sysctl settings:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv6.conf.all.disable_ipv6 = 1  
net.ipv6.conf.default.disable_ipv6 = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv6.conf.all.disable_ipv6=1  
# sysctl -w net.ipv6.conf.default.disable_ipv6=1  
# sysctl -w net.ipv6.route.flush=1
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.7 Ensure at least two name servers are configured if using DNS resolution (Automated)

Profile Applicability:

- STIG

Description:

For operating systems using DNS resolution, at least two name servers must be configured.

Rationale:

To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Audit:

Determine whether the system is using local or DNS name resolution with the following command:

```
# grep hosts /etc/nsswitch.conf  
hosts: files dns
```

If the DNS entry is missing from the host's line in the "/etc/nsswitch.conf" file, the "/etc/resolv.conf" file must be empty.

Verify the "/etc/resolv.conf" file is empty with the following command:

```
# ls -al /etc/resolv.conf  
-rw-r--r-- 1 root root 0 Aug 19 08:31 resolv.conf
```

If local host authentication is being used and the "/etc/resolv.conf" file is not empty, this is a finding.

If the DNS entry is found on the host's line of the "/etc/nsswitch.conf" file, verify the operating system is configured to use two or more name servers for DNS resolution. Determine the name servers used by the system with the following command:

```
# grep nameserver /etc/resolv.conf  
nameserver 192.168.1.2  
nameserver 192.168.1.3
```

If less than two lines are returned that are not commented out, this is a finding.

Remediation:

Configure the operating system to use two or more name servers for DNS resolution. By default, "NetworkManager" on RHEL 8 operating systems dynamically updates the /etc/resolv.conf file with the DNS settings from active "NetworkManager" connection profiles. However, this feature can be disabled to allow manual configurations.

If manually configuring DNS, edit the "/etc/resolv.conf" file to uncomment or add the two or more "nameserver" option lines with the IP address of local authoritative name servers. If local host resolution is being performed, the "/etc/resolv.conf" file must be empty. An empty "/etc/resolv.conf" file can be created as follows:

```
# echo -n > /etc/resolv.conf
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230316

Rule ID: SV-230316r627750_rule

STIG ID: RHEL-08-010680

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.8 Ensure Bluetooth is disabled (Automated)

Profile Applicability:

- STIG

Description:

Bluetooth must be disabled.

Rationale:

Without protection of communications with wireless peripherals, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read, altered, or used to compromise the operating system.

This requirement applies to wireless peripheral technologies (e.g., wireless mice, keyboards, displays, etc.) used with RHEL 8 operating systems. Wireless peripherals (e.g., Wi-Fi/Bluetooth/IR Keyboards, Mice, and Pointing Devices and Near Field Communications [NFC]) present a unique challenge by creating an open, unsecured port on a computer. Wireless peripherals must meet DoD requirements for wireless data transmission and be approved for use by the Authorizing Official (AO). Even though some wireless peripherals, such as mice and pointing devices, do not ordinarily carry information that need to be protected, modification of communications with these wireless peripherals may be used to compromise the operating system. Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of communications with wireless peripherals can be accomplished by physical means (e.g., employing physical barriers to wireless radio frequencies) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa. If the wireless peripheral is only passing telemetry data, encryption of the data may not be required.

Audit:

If the device or operating system does not have a Bluetooth adapter installed, this requirement is not applicable.

This requirement is not applicable to mobile devices (smartphones and tablets), where the use of Bluetooth is a local AO decision.

Determine if Bluetooth is disabled with the following command:

```
# grep bluetooth /etc/modprobe.d/*
/etc/modprobe.d/bluetooth.conf:install bluetooth /bin/true
```

If the Bluetooth driver blacklist entry is missing, a Bluetooth driver is determined to be in use, and the collaborative computing device has not been authorized for use, this is a finding.

Remediation:

Configure the operating system to disable the Bluetooth adapter when not in use. Build or modify the "/etc/modprobe.d/bluetooth.conf" file with the following line:

```
install bluetooth /bin/true
```

Reboot the system for the settings to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230507

Rule ID: SV-230507r627750_rule

STIG ID: RHEL-08-040111

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4 Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included in most distributions.

It is recommended that `rsyslog` be used for logging (with `logwatch` providing summarization) and `auditd` be used for auditing (with `aureport` providing summarization) to automatically monitor logs for intrusion attempts and other suspicious system behavior.

In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server via an encrypted connection. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices. Reference <<http://chrony.tuxfamily.org/>> manual page for more information on configuring chrony.

It is important that all logs described in this section be monitored on a regular basis and correlated to determine trends. A seemingly innocuous entry in one log could be more significant when compared to an entry in another log.

Note on log file permissions: There really isn't a "one size fits all" solution to the permissions on log files. Many sites utilize group permissions so that administrators who are in a defined security group, such as "wheel" do not have to elevate privileges to root in order to read log files. Also, if a third party log aggregation tool is used, it may need to have group permissions to read the log files, which is preferable to having it run setuid to root. Therefore, there are two remediation and audit steps for log file permissions. One is for systems that do not have a secured group method implemented that only permits root to read the log files (`root:root 600`). The other is for sites that do have such a setup and are designated as `root:securegrp 640` where `securegrp` is the defined security group (in some cases `wheel`).

4.1 Configure System Accounting (auditd)

System auditing, through `auditd`, allows system administrators to monitor their systems such that they can detect unauthorized access or modification of data. By default, `auditd` will audit SELinux AVC denials, system logins, account modifications, and authentication events. Events will be logged to `/var/log/audit/audit.log`. The recording of these events will use a modest amount of disk space on a system. If significantly more events are captured, additional on system or off system storage may need to be allocated.

The recommendations in this section implement an audit policy that produces large quantities of logged data. In some environments it can be challenging to store or process these logs and as such they are marked as Level 2 for both Servers and Workstations.

Note: For 64 bit systems that have `arch` as a rule parameter, you will need two rules: one for 64 bit and one for 32 bit.

Note: Systems may have been customized to change the default `UID_MIN`. To confirm the `UID_MIN` for your system, run the following command:

```
awk '/^s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' `UID_MIN` is not 1000, replace `audit>=1000` with `audit>=<UID_MIN` for your system> in the Audit and Remediation procedures.

Note: Once all configuration changes have been made to `/etc/audit/rules.d/audit.rules`, the `auditd` configuration must be reloaded with the following command:

```
# service auditd reload
```

4.1.1 Ensure auditing is enabled

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

4.1.1.1 Ensure auditd is installed (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

Description:

auditd is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk

Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Audit:

Run the following command and verify auditd is installed:

```
# rpm -q audit audit-libs
```

Remediation:

Run the following command to Install auditd

```
# dnf install audit audit-libs
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230411

Rule ID: SV-230411r744000_rule

STIG ID: RHEL-08-030180

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.</p>	●	●	●
v7	<p>6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p>6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

4.1.1.2 Ensure auditd service is enabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Turn on the `auditd` daemon to record system events.

Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Audit:

Run the following command to verify `auditd` is enabled:

```
# systemctl is-enabled auditd  
enabled
```

Verify result is "enabled".

Remediation:

Run the following command to enable `auditd`:

```
# systemctl --now enable auditd
```

Additional Information:

Additional methods of enabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Configure `grub2` so that processes that are capable of being audited can be audited even if they start up prior to `auditd` startup.

Rationale:

Audit events need to be captured on processes that start up prior to `auditd`, so that potential malicious activity cannot go undetected.

Audit:

Run the following command:

```
# grep -E 'kernelopts=(\s+\s+)*audit=1\b' /boot/grub2/grubenv
```

Output will include `audit=1`

Remediation:

Edit `/etc/default/grub` and add `audit=1` to `GRUB_CMDLINE_LINUX`:

```
GRUB_CMDLINE_LINUX="audit=1"
```

Run the following command to update the `grub2` configuration:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

Additional Information:

This recommendation is designed around the `grub2` bootloader, if another bootloader is in use in your environment enact equivalent settings.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.</p>	●	●	●
v7	<p>6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p>6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

4.1.1.4 Ensure audit_backlog_limit is sufficient (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The backlog limit has a default setting of 64

Rationale:

during boot if audit=1, then the backlog will hold 64 records. If more than 64 records are created during boot, audited records will be lost and potential malicious activity could go undetected.

Audit:

Run the following command and verify the `audit_backlog_limit` parameter is set to an appropriate size for your organization

```
# grep -E 'kernelopts=(\S+\s+)*audit_backlog_limit=\S+\b' /boot/grub2/grubenv
```

Validate that the line(s) returned contain a value for `audit_backlog_limit` and the value is sufficient for your organization.

Recommended that this value be 8192 or larger.

Remediation:

Edit `/etc/default/grub` and add `audit_backlog_limit=<BACKLOG_SIZE>` to `GRUB_CMDLINE_LINUX`:

Example:

```
GRUB_CMDLINE_LINUX="audit_backlog_limit=8192"
```

Run the following command to update the grub2 configuration:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.1.1.5 Ensure the audit service is configured to produce audit records (Automated)

Profile Applicability:

- STIG

Description:

Audit records must contain information to establish what type of events occurred, the source of events, where events occurred, and the outcome of events.

Rationale:

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in operating system audit logs provides a means of investigating an attack, recognizing resource utilization or capacity thresholds, or identifying an improperly configured RHEL 8 system.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00021, SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, SRG-OS-000122-GPOS-00063, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096, SRG-OS-000337-GPOS-00129, SRG-OS-000348-GPOS-00136, SRG-OS-000349-GPOS-00137, SRG-OS-000350-GPOS-00138, SRG-OS-000351-GPOS-00139, SRG-OS-000352-GPOS-00140, SRG-OS-000353-GPOS-00141, SRG-OS-000354-GPOS-00142, SRG-OS-000358-GPOS-00145, SRG-OS-000365-GPOS-00152, SRG-OS-000392-GPOS-00172, SRG-OS-000475-GPOS-00220

Audit:

Verify the audit service is configured to produce audit records with the following command:

```
# systemctl status auditd.service.  
  
auditd.service - Security Auditing Service  
Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; vendor  
preset: enabled)  
Active: active (running) since Tues 2020-12-11 12:56:56 EST; 4 weeks 0 days  
ago
```

If the audit service is not "active" and "running", this is a finding.

Remediation:

Configure the audit service to produce audit records containing the information needed to establish when (date and time) an event occurred with the following commands:

```
# systemctl enable auditd.service  
  
# systemctl start auditd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244542

Rule ID: SV-244542r743875_rule

STIG ID: RHEL-08-030181

Severity: CAT II

Vul ID: V-230297

Rule ID: SV-230297r627750_rule

STIG ID: RHEL-08-010560

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.2 Configure Data Retention

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, auditd will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, check your site policy for audit storage requirements.

4.1.2.1 Ensure audit log storage size is configured (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.

Rationale:

It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

Audit:

Run the following command and ensure output is in compliance with site policy:

```
# grep max_log_file /etc/audit/auditd.conf  
max_log_file = <MB>
```

Remediation:

Set the following parameter in */etc/audit/auditd.conf* in accordance with site policy:

```
max_log_file = <MB>
```

Additional Information:

The *max_log_file* parameter is measured in megabytes.

Other methods of log rotation may be appropriate based on site policy. One example is time-based rotation strategies which don't have native support in auditd configurations.

Manual audit of custom configurations should be evaluated for effectiveness and completeness.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

4.1.2.2 Ensure audit logs are not automatically deleted (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `max_log_file_action` setting determines how to handle the audit log file reaching the max file size. A value of `keep_logs` will rotate the logs but never delete old logs.

Rationale:

In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

Audit:

Run the following command and verify output matches:

```
# grep max_log_file_action /etc/audit/auditd.conf  
max_log_file_action = keep_logs
```

Remediation:

Set the following parameter in `/etc/audit/auditd.conf`:

```
max_log_file_action = keep_logs
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.	●	●	

4.1.2.3 Ensure system is disabled when audit logs are full (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `auditd` daemon can be configured to halt the system when the audit logs are full.

Rationale:

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

Audit:

Run the following commands and verify output matches:

```
# grep space_left_action /etc/audit/auditd.conf  
space_left_action = email  
  
# grep action_mail_acct /etc/audit/auditd.conf  
action_mail_acct = root  
  
# grep admin_space_left_action /etc/audit/auditd.conf  
admin_space_left_action = halt
```

Remediation:

Set the following parameters in `/etc/audit/auditd.conf`:

```
space_left_action = email  
action_mail_acct = root  
admin_space_left_action = halt
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			

4.1.2.4 Ensure the operating system allocates audit record storage capacity (Manual)

Profile Applicability:

- STIG

Description:

The operating system must allocate audit record storage capacity to store at least one week of audit records, when audit records are not immediately sent to a central audit record storage facility.

Rationale:

To ensure the operating system has a sufficient storage capacity in which to write the audit logs, the operating system needs to be able to allocate audit record storage capacity. The task of allocating audit record storage capacity is usually performed during initial installation of the operating system.

Audit:

Verify the operating system allocates audit record storage capacity to store at least one week of audit records when audit records are not immediately sent to a central audit record storage facility.

Determine to which partition the audit records are being written with the following command:

```
# grep log_file /etc/audit/auditd.conf  
log_file = /var/log/audit/audit.log
```

Check the size of the partition to which audit records are written (with the example being /var/log/audit/) with the following command:

```
# df -h /var/log/audit/  
/dev/sda2 24G 10.4G 13.6G 43% /var/log/audit
```

If the audit records are not written to a partition made specifically for audit records (/var/log/audit is a separate partition), determine the amount of space being used by other files in the partition with the following command:

```
# du -sh [audit_partition]  
1.8G /var/log/audit
```

If the audit record partition is not allocated for sufficient storage capacity, this is a finding.

Note: The partition size needed to capture a week of audit records is based on the activity level of the system and the total storage capacity available. Typically 10.0 GB of storage space for audit records should be sufficient.

Remediation:

Allocate enough storage capacity for at least one week of audit records when audit records are not immediately sent to a central audit record storage facility.

If audit records are stored on a partition made specifically for audit records, resize the partition with sufficient space to contain one week of audit records.

If audit records are not stored on a partition made specifically for audit records, a new partition with sufficient space will need to be created.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230476

Rule ID: SV-230476r627750_rule

STIG ID: RHEL-08-030660

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.	●	●	

4.1.2.5 Ensure the operating system has the packages required for offloading audit logs (Automated)

Profile Applicability:

- STIG

Description:

The operating system must have the packages required for offloading audit logs installed.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

The operating system's installation media provides "rsyslogd". "rsyslogd" is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Couple this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols), and you have a method to securely encrypt and off-load auditing.

Rsyslog provides three ways to forward message: the traditional UDP transport, which is extremely lossy but standard; the plain TCP based transport, which loses messages only during certain situations but is widely available; and the RELP transport, which does not lose messages but is currently available only as part of the rsyslogd 3.15.0 and above.

Examples of each configuration: UDP . @remotesystemname TCP . @@remotesystemname RELP . :omrelp:remotesystemname:2514 Note that a port number was given as there is no standard port for RELP.

Audit:

Verify the operating system has the packages required for offloading audit logs installed with the following commands:

```
# yum list installed rsyslog
rsyslog.x86_64 8.1911.0-3.el8 @AppStream
```

If the "rsyslog" package is not installed, ask the administrator to indicate how audit logs are being offloaded and what packages are installed to support it. If there is no evidence of audit logs being offloaded, this is a finding.

Remediation:

Configure the operating system to offload audit logs by installing the required packages with the following command:

```
# yum install rsyslog
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230477

Rule ID: SV-230477r627750_rule

STIG ID: RHEL-08-030670

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>8.9 Centralize Audit Logs</u> Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	<u>6.6 Deploy SIEM or Log Analytic tool</u> Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.		●	●

4.1.2.6 Ensure the operating system has the packages required for encrypting offloaded audit logs (Automated)

Profile Applicability:

- STIG

Description:

must have the packages required for encrypting offloaded audit logs installed.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

The operating system's installation media provides "rsyslogd". "rsyslogd" is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Couple this utility with "rsyslog-gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols), and you have a method to securely encrypt and off-load auditing.

Rsyslog provides three ways to forward message: the traditional UDP transport, which is extremely lossy but standard; the plain TCP based transport, which loses messages only during certain situations but is widely available; and the RELP transport, which does not lose messages but is currently available only as part of the rsyslogd 3.15.0 and above.

Examples of each configuration: UDP . @remotesystemname TCP . @@remotesystemname RELP . :omrelp:remotesystemname:2514 Note that a port number was given as there is no standard port for RELP.

Audit:

Verify the operating system has the packages required for encrypting offloaded audit logs installed with the following commands:

```
# yum list installed rsyslog-gnutls  
rsyslog-gnutls.x86_64 8.1911.0-3.el8 @AppStream
```

If the "rsyslog-gnutls" package is not installed, ask the administrator to indicate how audit logs are being encrypted during offloading and what packages are installed to support it. If there is no evidence of audit logs being encrypted during offloading, this is a finding.

Remediation:

Configure the operating system to encrypt offloaded audit logs by installing the required packages with the following command:

```
# yum install rsyslog-gnutls
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230478

Rule ID: SV-230478r744011_rule

STIG ID: RHEL-08-030680

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.6 Deploy SIEM or Log Analytic tool Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.		●	●

4.1.2.7 Ensure the audit system off-loads audit records onto a different system or media from the system being audited (Automated)

Profile Applicability:

- STIG

Description:

Audit records must be off-loaded onto a different system or storage media from the system being audited.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

The operating system's installation media provides "rsyslogd". "rsyslogd" is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Couple this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols), and you have a method to securely encrypt and off-load auditing.

Rsyslog provides three ways to forward message: the traditional UDP transport, which is extremely lossy but standard; the plain TCP based transport, which loses messages only during certain situations but is widely available; and the RELP transport, which does not lose messages but is currently available only as part of the rsyslogd 3.15.0 and above.

Examples of each configuration: UDP . @remotesystemname TCP . @@remotesystemname RELP . :omrelp:remotesystemname:2514 Note that a port number was given as there is no standard port for RELP.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify the audit system off-loads audit records onto a different system or media from the system being audited with the following command:

```
# grep @@ /etc/rsyslog.conf /etc/rsyslog.d/*.conf  
/etc/rsyslog.conf:.* @@[remoteloggingserver]:[port]
```

If a remote server is not configured, or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media. If there is no evidence that the audit logs are being off-loaded to another system or media, this is a finding.

Remediation:

Configure the operating system to off-load audit records onto a different system or media from the system being audited by specifying the remote logging server in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf" with the name or IP address of the log aggregation server.

```
*.* @@[remoteloggingserver]:[port]
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230479

Rule ID: SV-230479r627750_rule

STIG ID: RHEL-08-030690

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.6 Deploy SIEM or Log Analytic tool Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.		●	●

4.1.2.8 Ensure the audit system is configured to take an appropriate action when the internal event queue is full (Automated)

Profile Applicability:

- STIG

Description:

The operating system must take appropriate action when the internal event queue is full.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

The operating system's installation media provides "rsyslogd". "rsyslogd" is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Couple this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols), and you have a method to securely encrypt and off-load auditing.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify the audit system is configured to take an appropriate action when the internal event queue is full:

```
# grep -i overflow_action /etc/audit/auditd.conf  
overflow_action = syslog
```

If the value of the "overflow_action" option is not set to "syslog", "single", "halt", or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the transfer of the audit logs being off-loaded to another system or media takes appropriate action if the internal event queue becomes full, this is a finding.

Remediation:

Edit the /etc/audit/auditd.conf file and add or update the "overflow_action" option:

```
overflow_action = syslog
```

The audit daemon must be restarted for changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230480

Rule ID: SV-230480r627750_rule

STIG ID: RHEL-08-030700

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

*4.1.2.9 Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited
(Automated)*

Profile Applicability:

- STIG

Description:

The operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

The operating system's installation media provides "rsyslogd". "rsyslogd" is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Couple this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols), and you have a method to securely encrypt and off-load auditing.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify the operating system encrypts audit records off-loaded onto a different system or media from the system being audited with the following commands:

```
# grep -i '$DefaultNetstreamDriver' /etc/rsyslog.conf /etc/rsyslog.d/*.conf  
/etc/rsyslog.conf:$DefaultNetstreamDriver gtls
```

If the value of the "\$DefaultNetstreamDriver" option is not set to "gtls" or the line is commented out, this is a finding.

```
# grep -i '$ActionSendStreamDriverMode' /etc/rsyslog.conf  
/etc/rsyslog.d/*.conf  
/etc/rsyslog.conf:$ActionSendStreamDriverMode 1
```

If the value of the "\$ActionSendStreamDriverMode" option is not set to "1" or the line is commented out, this is a finding.

If either of the definitions above are set, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the transfer of the audit logs being off-loaded to another system or media is encrypted, this is a finding.

Remediation:

Configure the operating system to encrypt off-loaded audit records by setting the following options in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf":

```
$DefaultNetstreamDriver gtls  
$ActionSendStreamDriverMode 1
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230481

Rule ID: SV-230481r627750_rule

STIG ID: RHEL-08-030710

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.6 Deploy SIEM or Log Analytic tool Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.		●	●

4.1.2.10 Ensure the operating system authenticates the remote logging server for off-loading audit logs (Automated)

Profile Applicability:

- STIG

Description:

The operating system must authenticate the remote logging server for off-loading audit logs.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

The operating system's installation media provides "rsyslogd". "rsyslogd" is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Couple this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols), and you have a method to securely encrypt and off-load auditing.

"Rsyslog" supported authentication modes include: anon - anonymous authentication
x509/fingerprint - certificate fingerprint authentication
x509/certvalid - certificate validation only
x509/name - certificate validation and subject name authentication.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify the operating system authenticates the remote logging server for off-loading audit logs with the following command:

```
# grep -i '$ActionSendStreamDriverAuthMode' /etc/rsyslog.conf  
/etc/rsyslog.d/*.conf  
  
/etc/rsyslog.conf:$ActionSendStreamDriverAuthMode x509/name
```

If the value of the "\$ActionSendStreamDriverAuthMode" option is not set to "x509/name" or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the transfer of the audit logs being off-loaded to another system or media is encrypted, this is a finding.

Remediation:

Configure the operating system to authenticate the remote logging server for off-loading audit logs by setting the following option in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf":

```
$ActionSendStreamDriverAuthMode x509/name
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230482

Rule ID: SV-230482r627750_rule

STIG ID: RHEL-08-030720

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.6 Deploy SIEM or Log Analytic tool Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.		●	●

4.1.2.11 Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity (Automated)

Profile Applicability:

- STIG

Description:

The operating system must take action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

Rationale:

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Audit:

Verify the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity with the following commands:

```
# grep -w space_left /etc/audit/auditd.conf  
space_left = 25%
```

If the value of the "space_left" keyword is not set to "25%" or if the line is commented out, ask the System Administrator to indicate how the system is providing real-time alerts to the SA and ISSO.

If there is no evidence that real-time alerts are configured on the system, this is a finding.

Remediation:

Configure the operating system to initiate an action to notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity by adding/modifying the following line in the /etc/audit/auditd.conf file.

```
space_left = 25%
```

Note: Option names and values in the auditd.conf file are case insensitive.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230483

Rule ID: SV-230483r744014_rule

STIG ID: RHEL-08-030730

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.	●	●	

4.1.3 Ensure changes to system administration scope (`sudoers`) is collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor scope changes for system administrators. If the system has been properly configured to force system administrators to log in as themselves first and then use the `sudo` command to execute privileged commands, it is possible to monitor changes in scope.

The file `/etc/sudoers` will be written to when the file or its attributes have changed. The audit records will be tagged with the identifier "scope."

Rationale:

Changes in the `/etc/sudoers` file can indicate that an unauthorized change has been made to scope of system administrator activity.

Audit:

Run the following command to check the auditd `.rules` files:

```
# grep scope /etc/audit/rules.d/*.rules
```

Verify output of matches:

```
-w /etc/sudoers -p wa -k scope  
-w /etc/sudoers.d/ -p wa -k scope
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep scope
```

Verify output matches:

```
-w /etc/sudoers -p wa -k scope  
-w /etc/sudoers.d -p wa -k scope
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-scope.rules`

Add the following lines:

```
-w /etc/sudoers -p wa -k scope  
-w /etc/sudoers.d/ -p wa -k scope
```

Additional Information:

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●

4.1.4 Ensure the SA and ISSO are notified in the event of an audit processing failure (Automated)

Profile Applicability:

- STIG

Description:

The System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) must be alerted of an audit processing failure event.

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

Verify that the SA and ISSO (at a minimum) are notified in the event of an audit processing failure.

Check that the operating system notifies the SA and ISSO (at a minimum) in the event of an audit processing failure with the following command:

```
# grep action_mail_acct /etc/audit/auditd.conf  
action_mail_acct = root
```

If the value of the "action_mail_acct" keyword is not set to "root" and/or other accounts for security personnel, the "action_mail_acct" keyword is missing, or the retuned line is commented out, ask the system administrator to indicate how they and the ISSO are notified of an audit process failure. If there is no evidence of the proper personnel being notified of an audit processing failure, this is a finding.

Remediation:

Configure "auditd" service to notify the SA and ISSO in the event of an audit processing failure.

Edit the following line in "/etc/audit/auditd.conf" to ensure that administrators are notified via email for those situations:

```
action_mail_acct = root
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230388

Rule ID: SV-230388r627750_rule

STIG ID: RHEL-08-030020

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.5 Ensure the SA and ISSO are notified when the audit storage volume is full (Automated)

Profile Applicability:

- STIG

Description:

The operating system's System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) must be alerted when the audit storage volume is full.

Rationale:

It is critical that when the operating system is at risk of failing to process audit logs as required, it takes action to mitigate the failure. Audit processing failures include software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Responses to audit failure depend upon the nature of the failure mode.

When availability is an overriding concern, other approved actions in response to an audit failure are as follows:

1. If the failure was caused by the lack of audit record storage capacity, the operating system must continue generating audit records if possible (automatically restarting the audit service if necessary) and overwriting the oldest audit records in a first-in-first-out manner.
2. If audit records are sent to a centralized collection server and communication with this server is lost or the server fails, the operating system must queue audit records locally until communication is restored or until the audit records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local audit data with the collection server.

Audit:

Verify that the SA and ISSO (at a minimum) are notified when the audit storage volume is full.

Check which action the operating system takes when the audit storage volume is full with the following command:

```
# grep max_log_file_action /etc/audit/auditd.conf  
max_log_file_action=syslog
```

If the value of the "max_log_file_action" option is set to "ignore", "rotate", or "suspend", or the line is commented out, ask the system administrator to indicate how the system takes appropriate action when an audit storage volume is full. If there is no evidence of appropriate action, this is a finding``

Remediation:

Configure the operating system to notify the System Administrator (SA) and Information System Security Officer (ISSO) when the audit storage volume is full by configuring the "max_log_file_action" parameter in the "/etc/audit/auditd.conf" file with the a value of "syslog" or "keep_logs":

```
max_log_file_action = syslog
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230391

Rule ID: SV-230391r743998_rule

STIG ID: RHEL-08-030050

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.			

4.1.6 Ensure an audit event is generated for any successful/unsuccessful use of the "chage" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the chage command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chage" command is used to change or view user password expiry information.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "chage" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w chage /etc/audit/audit.rules
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-chage
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "chage" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-chage
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230418

Rule ID: SV-230418r627750_rule

STIG ID: RHEL-08-030250

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.7 Ensure the operating system is configured to audit the execution of the "fremovexattr" system call (Automated)

Profile Applicability:

- STIG

Description:

The audit system must be configured to audit any usage of the fremovexattr system call.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). "Fremovexattr" is a system call that removes extended attributes. This is used for removal of extended attributes from a file.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000462-GPOS-00206, SRG-OS-000463-GPOS-00207, SRG-OS-000471-GPOS-00215, SRG-OS-000474-GPOS-00219, SRG-OS-000466-GPOS-00210

Audit:

Verify if the operating system is configured to audit the execution of the "fremovexattr" system call, by running the following command:

```
# grep -w fremovexattr /etc/audit/audit.rules  
  
-a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=unset -k perm_mod  
-a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid!=unset -k perm_mod  
  
-a always,exit -F arch=b32 -S fremovexattr -F auid=0 -k perm_mod  
-a always,exit -F arch=b64 -S fremovexattr -F auid=0 -k perm_mod
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the operating system to audit the execution of the "fremovexattr" system call by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=unset -k perm_mod  
-a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid!=unset -k perm_mod  
  
-a always,exit -F arch=b32 -S fremovexattr -F auid=0 -k perm_mod  
-a always,exit -F arch=b64 -S fremovexattr -F auid=0 -k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230417

Rule ID: SV-230417r627750_rule

STIG ID: RHEL-08-030240

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.8 Ensure the operating system is configured to audit the execution of the "fsetxattr" system call (Automated)

Profile Applicability:

- STIG

Description:

The audit system must be configured to audit any usage of the fsetxattr system call.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). "Fsetxattr" is a system call used to set an extended attribute value. This is used to set extended attributes on a file.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The auid representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000462-GPOS-00206, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215, SRG-OS-000474-GPOS-00219

Audit:

Verify if the operating system is configured to audit the execution of the "fsetxattr" system call, by running the following command:

```
# grep -w fsetxattr /etc/audit/audit.rules

-a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=unset -k
perm_mod
-a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=unset -k
perm_mod

-a always,exit -F arch=b32 -S fsetxattr -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S fsetxattr -F auid=0 -k perm_mod
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the operating system to audit the execution of the "fsetxattr" system call, by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=unset -k perm_mod  
-a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=unset -k perm_mod  
  
-a always,exit -F arch=b32 -S fsetxattr -F auid=0 -k perm_mod  
-a always,exit -F arch=b64 -S fsetxattr -F auid=0 -k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230416

Rule ID: SV-230416r627750_rule

STIG ID: RHEL-08-030230

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.9 Ensure the operating system is configured to audit the execution of the "lsetxattr" system call (Automated)

Profile Applicability:

- STIG

Description:

The audit system must be configured to audit any usage of the lsetxattr system call.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). "Lsetxattr" is a system call used to set an extended attribute value. This is used to set extended attributes on a symbolic link.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000462-GPOS-00206, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215, SRG-OS-000474-GPOS-00219

Audit:

Verify if the operating system is configured to audit the execution of the "lsetxattr" system call, by running the following command:

```
# grep -w lsetxattr /etc/audit/audit.rules

-a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=unset -k
perm_mod
-a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=unset -k
perm_mod

-a always,exit -F arch=b32 -S lsetxattr -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S lsetxattr -F auid=0 -k perm_mod
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the operating system to audit the execution of the "lsetxattr" system call, by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=unset -k perm_mod  
-a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=unset -k perm_mod  
  
-a always,exit -F arch=b32 -S lsetxattr -F auid=0 -k perm_mod  
-a always,exit -F arch=b64 -S lsetxattr -F auid=0 -k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230415

Rule ID: SV-230415r627750_rule

STIG ID: RHEL-08-030220

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.10 Ensure the operating system is configured to audit the execution of the "removexattr" system call (Automated)

Profile Applicability:

- STIG

Description:

The audit system must be configured to audit any usage of the removexattr system call.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). "Removexattr" is a system call that removes extended attributes.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000462-GPOS-00206, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215, SRG-OS-000474-GPOS-00219, SRG-OS-000466-GPOS-00210

Audit:

Verify if the operating system is configured to audit the execution of the "removexattr" system call, by running the following command:

```
# grep -w removexattr /etc/audit/audit.rules
-a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid!=unset -k perm_mod

-a always,exit -F arch=b32 -S removexattr -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S removexattr -F auid=0 -k perm_mod
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the operating system to audit the execution of the "removexattr" system call, by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=unset -k perm_mod  
-a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid!=unset -k perm_mod  
  
-a always,exit -F arch=b32 -S removexattr -F auid=0 -k perm_mod  
-a always,exit -F arch=b64 -S removexattr -F auid=0 -k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230414

Rule ID: SV-230414r627750_rule

STIG ID: RHEL-08-030210

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.11 Ensure the operating system is configured to audit the execution of the "lremovexattr" system call (Automated)

Profile Applicability:

- STIG

Description:

The audit system must be configured to audit any usage of the lremovexattr system call.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). "Lremovexattr" is a system call that removes extended attributes. This is used for removal of extended attributes from symbolic links.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000462-GPOS-00206, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215, SRG-OS-000474-GPOS-00219, SRG-OS-000466-GPOS-00210

Audit:

Verify if the operating system is configured to audit the execution of the "lremovexattr" system call, by running the following command:

```
# grep -w lremovexattr /etc/audit/audit.rules
-a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S lremovexattr -F auid>=1000 -F auid!=unset -k perm_mod

-a always,exit -F arch=b32 -S lremovexattr -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S lremovexattr -F auid=0 -k perm_mod
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the operating system to audit the execution of the "lremovexattr" system call, by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=unset -k perm_mod  
-a always,exit -F arch=b64 -S lremovexattr -F auid>=1000 -F auid!=unset -k perm_mod  
  
-a always,exit -F arch=b32 -S lremovexattr -F auid=0 -k perm_mod  
-a always,exit -F arch=b64 -S lremovexattr -F auid=0 -k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230413

Rule ID: SV-230413r627750_rule

STIG ID: RHEL-08-030200

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.12 Ensure the operating system generates audit records when successful/unsuccessful attempts to use the "su" command by performing the following command to check the file system rules in "/etc/audit/audit.rules" (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the su command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "su" command allows a user to run commands with a substitute user and group ID.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000064-GPOS-0003, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "su" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w /usr/bin/su /etc/audit/audit.rules  
-a always,exit -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=unset -k  
privileged-priv_change
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "su" command occur by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=unset -k  
privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230412

Rule ID: SV-230412r627750_rule

STIG ID: RHEL-08-030190

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.			

4.1.13 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/sudoers.d/.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, CCI-002884, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
# grep /etc/sudoers.d/ /etc/audit/audit.rules  
-w /etc/sudoers.d/ -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/sudoers.d/ -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230410

Rule ID: SV-230410r627750_rule

STIG ID: RHEL-08-030172

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

4.1.14 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/sudoers.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, CCI-002884, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
# grep /etc/sudoers /etc/audit/audit.rules  
-w /etc/sudoers -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/sudoers -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230409

Rule ID: SV-230409r627750_rule

STIG ID: RHEL-08-030171

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

4.1.15 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
# grep /etc/gshadow /etc/audit/audit.rules  
-w /etc/gshadow -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/gshadow -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230407

Rule ID: SV-230407r627750_rule=

STIG ID: RHEL-08-030160

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

4.1.16 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/security/opasswd.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, SRG-OS-000476-GPOS-00221

Audit:

Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
# grep /etc/security/opasswd /etc/audit/audit.rules  
-w /etc/security/opasswd -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/security/opasswd -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230405

Rule ID: SV-230405r627750_rule

STIG ID: RHEL-08-030140

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.17 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
# grep /etc/shadow /etc/audit/audit.rules  
-w /etc/shadow -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/shadow -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230404

Rule ID: SV-230404r627750_rule

STIG ID: RHEL-08-030130

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.18 Ensure the audit system prevents unauthorized changes to logon UIDs (Automated)

Profile Applicability:

- STIG

Description:

The audit system must protect logon UIDs from unauthorized change.

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit system activity.

In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. A system reboot would be noticeable and a system administrator could then investigate the unauthorized changes.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit system prevents unauthorized changes to logon UIDs with the following command:

```
# grep -i immutable /etc/audit/audit.rules  
--loginuid-immutable
```

If the login UIDs are not set to be immutable by adding the "--loginuid-immutable" option to the "/etc/audit/audit.rules", this is a finding.

Remediation:

Configure the audit system to set the logon UIDs to be immutable by adding the following line to "/etc/audit/rules.d/audit.rules"

```
--loginuid-immutable
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230403

Rule ID: SV-230403r627750_rule

STIG ID: RHEL-08-030122

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.19 Ensure the audit system prevents unauthorized changes (Automated)

Profile Applicability:

- STIG

Description:

The audit system must protect auditing rules from unauthorized change.

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit system activity.

In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. A system reboot would be noticeable and a system administrator could then investigate the unauthorized changes.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit system prevents unauthorized changes with the following command:

```
# grep "^\s*[^\#]" /etc/audit/audit.rules | tail -1  
-e 2
```

If the audit system is not set to be immutable by adding the "-e 2" option to the "/etc/audit/audit.rules", this is a finding.

Remediation:

Configure the audit system to set the audit rules to be immutable by adding the following line to "/etc/audit/rules.d/audit.rules"

```
-e 2
```

Note: Once set, the system must be rebooted for auditing to be changed. It is recommended to add this option as the last step in securing the system.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230402

Rule ID: SV-230402r627750_rule

STIG ID: RHEL-08-030121

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.20 Ensure the operating system takes the appropriate action when the audit storage volume is full (Automated)

Profile Applicability:

- STIG

Description:

The audit system must take appropriate action when the audit storage volume is full.

Rationale:

It is critical that when the operating system is at risk of failing to process audit logs as required, it takes action to mitigate the failure. Audit processing failures include software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Responses to audit failure depend upon the nature of the failure mode.

When availability is an overriding concern, other approved actions in response to an audit failure are as follows:

1. If the failure was caused by the lack of audit record storage capacity, the operating system must continue generating audit records if possible (automatically restarting the audit service if necessary) and overwriting the oldest audit records in a first-in-first-out manner.
2. If audit records are sent to a centralized collection server and communication with this server is lost or the server fails, the operating system must queue audit records locally until communication is restored or until the audit records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local audit data with the collection server.

Audit:

Verify the operating system takes the appropriate action when the audit storage volume is full.

Check that the operating system takes the appropriate action when the audit storage volume is full with the following command:

```
# grep disk_full_action /etc/audit/auditd.conf  
disk_full_action = HALT
```

If the value of the "disk_full_action" option is not "SYSLOG", "SINGLE", or "HALT", or the line is commented out, ask the system administrator to indicate how the system takes appropriate action when an audit storage volume is full. If there is no evidence of appropriate action, this is a finding.

Remediation:

Configure the operating system to shut down by default upon audit failure (unless availability is an overriding concern).

Add or update the following line (depending on configuration "disk_full_action" can be set to "SYSLOG" or "SINGLE" depending on configuration) in "/etc/audit/auditd.conf" file:

```
disk_full_action = HALT
```

If availability has been determined to be more important, and this decision is documented with the ISSO, configure the operating system to notify system administration staff and ISSO staff in the event of an audit processing failure by setting the "disk_full_action" to "SYSLOG".

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230392

Rule ID: SV-230392r627750_rule

STIG ID: RHEL-08-030060

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

4.1.21 Ensure the operating system takes the appropriate action when the audit storage volume is full (Automated)

Profile Applicability:

- STIG

Description:

The audit system must take appropriate action when the audit storage volume is full.

Rationale:

It is critical that when the operating system is at risk of failing to process audit logs as required, it takes action to mitigate the failure. Audit processing failures include software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Responses to audit failure depend upon the nature of the failure mode.

When availability is an overriding concern, other approved actions in response to an audit failure are as follows:

1. If the failure was caused by the lack of audit record storage capacity, the operating system must continue generating audit records if possible (automatically restarting the audit service if necessary) and overwriting the oldest audit records in a first-in-first-out manner.
2. If audit records are sent to a centralized collection server and communication with this server is lost or the server fails, the operating system must queue audit records locally until communication is restored or until the audit records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local audit data with the collection server.

Audit:

Verify the operating system takes the appropriate action when the audit storage volume is full.

Check that the operating system takes the appropriate action when the audit storage volume is full with the following command:

```
# grep disk_full_action /etc/audit/auditd.conf  
disk_full_action = HALT
```

If the value of the "disk_full_action" option is not "SYSLOG", "SINGLE", or "HALT", or the line is commented out, ask the system administrator to indicate how the system takes appropriate action when an audit storage volume is full. If there is no evidence of appropriate action, this is a finding.

Remediation:

Configure the operating system to shut down by default upon audit failure (unless availability is an overriding concern).

Add or update the following line (depending on configuration "disk_full_action" can be set to "SYSLOG" or "SINGLE" depending on configuration) in "/etc/audit/auditd.conf" file:

```
disk_full_action = HALT
```

If availability has been determined to be more important, and this decision is documented with the ISSO, configure the operating system to notify system administration staff and ISSO staff in the event of an audit processing failure by setting the "disk_full_action" to "SYSLOG".

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230392

Rule ID: SV-230392r627750_rule

STIG ID: RHEL-08-030060

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

4.1.22 Ensure login and logout events are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor login and logout events. The parameters below track changes to files associated with login/logout events.

- The file `/var/log/lastlog` maintains records of the last time a user successfully logged in.
- The `/var/run/faillock/` directory maintains records of login failures via the `pam_faillock` module.

Rationale:

Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Audit:

Run the following commands:

```
# grep logins /etc/audit/rules.d/*.rules  
# auditctl -l | grep logins
```

Verify output of both includes:

```
-w /var/log/lastlog -p wa -k logins  
-w /var/run/faillock/ -p wa -k logins
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-logins.rules`

Add the following lines:

```
-w /var/log/lastlog -p wa -k logins  
-w /var/run/faillock/ -p wa -k logins
```

Additional Information:

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.	●	●	●
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	●	●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.23 Ensure the operating system takes the appropriate action when an audit processing failure occurs (Automated)

Profile Applicability:

- STIG

Description:

The operating system must take appropriate action when an audit processing failure occurs.

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

Ensure the operating system takes the appropriate action when an audit processing failure occurs.

Check that the operating system takes the appropriate action when an audit processing failure occurs with the following command:

```
# grep disk_error_action /etc/audit/auditd.conf  
disk_error_action = HALT
```

If the value of the "disk_error_action" option is not "SYSLOG", "SINGLE", or "HALT", or the line is commented out, ask the system administrator to indicate how the system takes appropriate action when an audit process failure occurs. If there is no evidence of appropriate action, this is a finding.

Remediation:

Configure the operating system to shut down by default upon audit failure (unless availability is an overriding concern).

Add or update the following line (depending on configuration "disk_error_action" can be set to "SYSLOG" or "SINGLE" depending on configuration) in "/etc/audit/auditd.conf" file:

```
disk_error_action = HALT
```

If availability has been determined to be more important, and this decision is documented with the ISSO, configure the operating system to notify system administration staff and ISSO staff in the event of an audit processing failure by setting the "disk_error_action" to "SYSLOG".

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230390

Rule ID: SV-230390r627750_rule

STIG ID: RHEL-08-030040

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.24 Ensure session initiation information is collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file `/var/run/utmp` tracks all currently logged in users.

All audit records will be tagged with the identifier "session." The `/var/log/wtmp` file tracks logins, logouts, shutdown, and reboot events. The file `/var/log/btmp` keeps track of failed login attempts and can be read by entering the command `/usr/bin/last -f /var/log/btmp`. All audit records will be tagged with the identifier "logins."

Rationale:

Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

Audit:

Run the following command to check the `auditd .rules` files:

```
# grep -E '(session|logins)' /etc/audit/rules.d/*.rules
```

Verify output includes:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep -E '(session|logins)'
```

Verify output includes:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-session.rules`

Add the following lines:

```
-w /var/run/utmp -p wa -k session  
-w /var/log/wtmp -p wa -k logins  
-w /var/log/btmp -p wa -k logins
```

Additional Information:

The `last` command can be used to read `/var/log/wtmp` (`last` with no parameters) and `/var/run/utmp` (`last -f /var/run/utmp`)

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.25 Ensure events that modify date and time information are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the `adjtimex` (tune kernel clock), `settimeofday` (Set time, using timeval and timezone structures) `stime` (using seconds since 1/1/1970) or `clock_settime` (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the `/var/log/audit.log` file upon exit, tagging the records with the identifier "time-change"

Rationale:

Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Audit:

On a 32 bit system run the following commands:

```
# grep time-change /etc/audit/rules.d/*.rules
# auditctl -l | grep time-change
```

Verify output of both matches:

```
-a always,exit -F arch=b32 -S adjtimex -S gettimeofday -S stime -k time-
change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
```

On a 64 bit system run the following commands:

```
# grep time-change /etc/audit/rules.d/*.rules
# auditctl -l | grep time-change
```

Verify output of both matches:

```
-a always,exit -F arch=b64 -S adjtimex -S gettimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S gettimeofday -S stime -k time-
change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
```

Remediation:

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-time_change.rules

Add the following lines:

```
-a always,exit -F arch=b32 -S adjtimex -S settimofday -S stime -k time-change  
-a always,exit -F arch=b32 -S clock_settime -k time-change  
-w /etc/localtime -p wa -k time-change
```

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-time_change.rules

Add the following lines:

```
-a always,exit -F arch=b64 -S adjtimex -S settimofday -k time-change  
-a always,exit -F arch=b32 -S adjtimex -S settimofday -S stime -k time-change  
-a always,exit -F arch=b64 -S clock_settime -k time-change  
-a always,exit -F arch=b32 -S clock_settime -k time-change  
-w /etc/localtime -p wa -k time-change
```

Additional Information:

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

4.1.26 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor SELinux/AppArmor mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or /etc/apparmor and /etc/apparmor.d directories.

Rationale:

Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Audit:

Run the following commands:

```
# grep MAC-policy /etc/audit/rules.d/*.rules  
# auditctl -l | grep MAC-policy
```

Verify output of both matches:

```
-w /etc/selinux/ -p wa -k MAC-policy  
-w /usr/share/selinux/ -p wa -k MAC-policy
```

Remediation:

Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-MAC_policy.rules

Add the following lines:

```
-w /etc/selinux/ -p wa -k MAC-policy  
-w /usr/share/selinux/ -p wa -k MAC-policy
```

Additional Information:

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			

4.1.27 Ensure events that modify the system's network environment are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Record changes to network environment files or system calls. The below parameters monitor the `sethostname` (set the systems host name) or `setdomainname` (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the `/etc/issue` and `/etc/issue.net` files (messages displayed pre-login), `/etc/hosts` (file containing host names and associated IP addresses) and `/etc/sysconfig/network` (directory containing network interface scripts and configurations) files.

Rationale:

Monitoring `sethostname` and `setdomainname` will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The `/etc/hosts` file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring `/etc/issue` and `/etc/issue.net` is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring `/etc/sysconfig/network` is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier "system-locale."

Audit:

On a 32 bit system run the following commands:

```
# grep system-locale /etc/audit/rules.d/*.rules  
# auditctl -l | grep system-locale
```

Verify output of both matches:

```
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale  
-w /etc/issue -p wa -k system-locale  
-w /etc/issue.net -p wa -k system-locale  
-w /etc/hosts -p wa -k system-locale  
-w /etc/sysconfig/network -p wa -k system-locale
```

On a 64 bit system run the following commands:

```
# grep system-locale /etc/audit/rules.d/*.rules  
# auditctl -l | grep system-locale
```

Verify output of both matches:

```
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale  
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale  
-w /etc/issue -p wa -k system-locale  
-w /etc/issue.net -p wa -k system-locale  
-w /etc/hosts -p wa -k system-locale  
-w /etc/sysconfig/network -p wa -k system-locale
```

Remediation:

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-system_local.rules

Add the following lines:

```
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale  
-w /etc/issue -p wa -k system-locale  
-w /etc/issue.net -p wa -k system-locale  
-w /etc/hosts -p wa -k system-locale  
-w /etc/sysconfig/network -p wa -k system-locale
```

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-system_local.rules

Add the following lines:

```
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale  
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale  
-w /etc/issue -p wa -k system-locale  
-w /etc/issue.net -p wa -k system-locale  
-w /etc/hosts -p wa -k system-locale  
-w /etc/sysconfig/network -p wa -k system-locale
```

Additional Information:

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

4.1.28 Ensure discretionary access control permission modification events are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The `chmod`, `fchmod` and `fchmodat` system calls affect the permissions associated with a file. The `chown`, `fchown`, `fchownat` and `lchown` system calls affect owner and group attributes on a file. The `setxattr`, `lsetxattr`, `fsetxattr` (set extended file attributes) and `removexattr`, `lremovexattr`, `fremovexattr` (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (`auid >= 1000`) and will ignore Daemon events (`auid = 4294967295`). All audit records will be tagged with the identifier "perm_mod."

Note: Systems may have been customized to change the default `UID_MIN`. To confirm the `UID_MIN` for your system, run the following command:

```
# awk '/^s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' `UID_MIN` is not `1000`, replace `audit>=1000` with `audit>=<UID_MIN` for your system in the Audit and Remediation procedures.

Rationale:

Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Audit:

On a 32 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep perm_mod /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295
-k perm_mod
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep perm_mod
```

Verify output matches:

```
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid==1
-F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F
auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid==1 -F key=perm_mod
```

On a 64 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep perm_mod /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295
-k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295
-k perm_mod
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep auditctl -l | grep perm_mod
```

Verify output matches:

```
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F auid>=1000 -F auid!=-1 -F key=perm_mod
```

Remediation:

For 32 bit systems edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-perm_mod.rules

Add the following lines:

```
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
```

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-perm_mod.rules

Add the following lines:

```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
```

Additional Information:

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.	●	●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.	●	●	●

4.1.29 Ensure unsuccessful unauthorized file access attempts are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (`creat`), opening (`open`, `openat`) and truncation (`truncate`, `ftruncate`) of files. An audit log record will only be written if the user is a non-privileged user (`auid >= 1000`), is not a Daemon event (`auid=4294967295`) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier "access."

Note: Systems may have been customized to change the default UID_MIN. To confirm the UID_MIN for your system, run the following command:

```
awk '/^s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' UID_MIN is not 1000, replace `audit>=1000` with `audit>=<UID_MIN` for your system in the Audit and Remediation procedures.

Rationale:

Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Audit:

On a 32 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep access /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep access
```

Verify output matches:

```
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=--1 -k access  
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=--1 -k access
```

On a 64 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep access /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access  
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access  
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access  
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep access
```

Verify output matches:

```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=--1 -k access  
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=--1 -k access  
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=--1 -k access  
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=--1 -k access
```

Remediation:

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-access.rules

Add the following lines:

```
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access  
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
```

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-access.rules

Add the following lines:

```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access  
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access  
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access  
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S  
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
```

Additional Information:

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

4.1.30 Ensure events that modify user/group information are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier "identity" in the audit log file.

Rationale:

Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Audit:

Run the following command to check the auditd .rules files:

```
# grep identity /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep identity
```

Verify the output matches:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

Remediation:

Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-identity.rules

Add the following lines:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

Additional Information:

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	●	●	

4.1.31 Ensure successful file system mounts are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor the use of the `mount` system call. The `mount` (and `umount`) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the `mount` system call is used by a non-privileged user.

Rationale:

It is highly unusual for a non privileged user to `mount` file systems to the system. While tracking `mount` commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful `open`, `creat` and `truncate` system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

Note: Systems may have been customized to change the default `UID_MIN`. To confirm the `UID_MIN` for your system, run the following command:

```
awk '/^s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' `UID_MIN` is not 1000, replace `audit>=1000` with `audit>=<UID_MIN` for your system in the Audit and Remediation procedures.

Audit:

On a 32 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep mounts /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k  
mounts
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep mounts
```

Verify output matches:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -k mounts
```

On a 64 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep mounts /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k  
mounts  
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k  
mounts
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep mounts
```

Verify output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=-1 -k mounts  
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -k mounts
```

Remediation:

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-mounts.rules

Add the following lines:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k  
mounts
```

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-mounts.rules

Add the following lines:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k  
mounts  
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k  
mounts
```

Additional Information:

This tracks successful and unsuccessful mount commands. File system mounts do not have to come from external media and this action still does not verify write (e.g. CD ROMS). Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.32 Ensure use of privileged commands is collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor privileged programs (those that have the setuid and/or setgid bit set on execution) to determine if unprivileged users are running these commands.

Rationale:

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

Audit:

Run the following command replacing <partition> with a list of partitions where programs can be executed from on your system:

```
# find <partition> -xdev \( -perm -4000 -o -perm -2000 \|) -type f | awk  
'{print "-a always,exit -F path=" $1 " -F perm=x -F auid>=" $(awk  
'/^\\s*UID_MIN/{print $2}' /etc/login.defs)"' -F auid!=4294967295 -k  
privileged" }'
```

Verify all resulting lines are a .rules file in /etc/audit/rules.d/ and the output of auditctl -l.

Note: The .rules file output will be auid!=--1 not auid!=4294967295

Remediation:

To remediate this issue, the system administrator will have to execute a find command to locate all the privileged programs and then add an audit line for each one of them.

The audit parameters associated with this are as follows:

- -F path=" \$1 " - will populate each file name found through the find command and processed by awk.
- -F perm=x - will write an audit record if the file is executed.
- -F audit>=1000 - will write a record if the user executing the command is not a privileged user.
- -F auid!= 4294967295 - will ignore Daemon events

All audit records should be tagged with the identifier "privileged".

Run the following command replacing with a list of partitions where programs can be executed from on your system:

```
# find <partition> -xdev \(\ -perm -4000 -o -perm -2000 \) -type f | awk  
'{print "-a always,exit -F path=" $1 " -F perm=x -F auid>='$(awk  
'/^s*UID_MIN/{print $2}' /etc/login.defs)"' -F auid!=4294967295 -k  
privileged" }'
```

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules` and add all resulting lines to the file.

Example:

```
# find / -xdev \(\ -perm -4000 -o -perm -2000 \) -type f | awk '{print "-a  
always,exit -F path=" $1 " -F perm=x -F auid>='$(awk '/^s*UID_MIN/{print  
$2}' /etc/login.defs)"' -F auid!=4294967295 -k privileged" }' >>  
/etc/audit/rules.d/50-privileged.rules
```

Additional Information:

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.33 Ensure file deletion events by users are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for the `unlink` (remove a file), `unlinkat` (remove a file attribute), `rename` (rename a file) and `renameat` (rename a file attribute) system calls and tags them with the identifier "delete".

Note: Systems may have been customized to change the default `UID_MIN`. To confirm the `UID_MIN` for your system, run the following command:

```
awk '/^s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' `UID_MIN` is not 1000, replace `audit>=1000` with `audit>=<UID_MIN` for your `system>` in the Audit and Remediation procedures.

Rationale:

Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

Audit:

On a 32 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep delete /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=4294967295 -k delete
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep delete
```

Verify output matches:

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=4294967295 -k delete
```

On a 64 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep delete /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=4294967295 -k delete  
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=4294967295 -k delete
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep delete
```

Verify output matches:

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid==1 -k delete  
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid==1 -k delete
```

Remediation:

For 32 bit systems edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-deletion.rules

Add the following lines:

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=4294967295 -k delete
```

For 64 bit systems edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-deletion.rules

Add the following lines:

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=4294967295 -k delete  
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=4294967295 -k delete
```

Additional Information:

At a minimum, configure the audit system to collect file deletion events for all users and root.

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	13 Data Protection Data Protection			

4.1.34 Ensure kernel module loading and unloading is collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor the loading and unloading of kernel modules. The programs `insmod` (install a kernel module), `rmmod` (remove a kernel module), and `modprobe` (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The `init_module` (load a module) and `delete_module` (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of "modules".

Rationale:

Monitoring the use of `insmod`, `rmmod` and `modprobe` could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the `init_module` and `delete_module` system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Audit:

On a 32 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep modules /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep modules
```

Verify output matches:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module,delete_module -F key=modules
```

On a 64 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep modules /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep modules
```

Verify output matches:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module,delete_module -F key=modules
```

Remediation:

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-modules.rules

Add the following lines:

```
-w /sbin/insmod -p x -k modules  
-w /sbin/rmmod -p x -k modules  
-w /sbin/modprobe -p x -k modules  
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
```

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-modules.rules

Add the following lines:

```
-w /sbin/insmod -p x -k modules  
-w /sbin/rmmod -p x -k modules  
-w /sbin/modprobe -p x -k modules  
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
```

Additional Information:

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.35 Ensure system administrator actions (sudolog) are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor the `sudo` log file. If the system has been properly configured to disable the use of the `su` command and force all administrators to have to log in first and then use `sudo` to execute privileged commands, then all administrator commands will be logged to `/var/log/sudo.log`. Any time a command is executed, an audit event will be triggered as the `/var/log/sudo.log` file will be opened for write and the executed administration command will be written to the log.

Rationale:

Changes in `/var/log/sudo.log` indicate that an administrator has executed a command or the log file itself has been tampered with. Administrators will want to correlate the events written to the audit trail with the records written to `/var/log/sudo.log` to verify if unauthorized commands have been executed.

Audit:

Run the following commands:

```
# grep -P -- "^\h*-w\h+$ (grep -r logfile /etc/sudoers* | sed -e 's/.*logfile=//;s/,? .*//' | tr -d '\"') \h+-p\h+wa\h+-k\h+\H+\h* (\h+.* )? $" /etc/audit/rules.d/*.rules

# auditctl -l | grep -P -- "^\h*-w\h+$ (grep -r logfile /etc/sudoers* | sed -e 's/.*logfile=//;s/,? .*//' | tr -d '\"') \h+-p\h+wa\h+-k\h+\H+\h* (\h+.* )? $"
```

Verify output of both matches the output of the following command, and the the output includes a file path

```
echo "-w $(grep -r logfile /etc/sudoers* | sed -e 's/.*logfile=//;s/,? .*//' | tr -d '\"') -p wa -k actions"
```

Example Output:

```
-w /var/log/sudo.log -p wa -k actions
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules` and add the following line:

```
-w <Path to sudo logfile> -p wa -k actions
```

Example:

Run the following command

```
# echo "-w $(grep -r logfile /etc/sudoers* | sed -e 's/.*logfile=//;s/,? .*//' | tr -d \"') -p wa -k actions" >> /etc/audit/rules.d/50-actions.rules
```

Additional Information:

The system must be configured with `su` disabled (See Recommendation: "Ensure access to the `su` command is restricted") to force all command execution through `sudo`. This will not be effective on the console, as administrators can log in as root.

Reloading the `audited` config to set active settings may require a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.			

4.1.36 Ensure the audit configuration is immutable (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Set system audit so that audit rules cannot be modified with `auditctl`. Setting the flag "-e 2" forces audit to be put in immutable mode. Audit changes can only be made on system reboot.

Rationale:

In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. Users would most likely notice a system reboot and that could alert administrators of an attempt to make unauthorized audit changes.

Audit:

Run the following command and verify output matches:

```
# grep "^\s*[^#]" /etc/audit/rules.d/*.rules | tail -1  
-e 2
```

Remediation:

Edit or create the file `/etc/audit/rules.d/99-finalize.rules` and add the following line at the end of the file:

```
-e 2
```

Additional Information:

This setting will ensure reloading the auditd config to set active settings requires a system reboot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.</p>		●	●
v7	<p>6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p>6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

4.1.37 Ensure the operating system audits the execution of privileged functions (Automated)

Profile Applicability:

- STIG

Description:

The audit system must be configured to audit the execution of privileged functions and prevent all software from executing at higher privilege levels than users executing the software.

Rationale:

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Satisfies: SRG-OS-000326-GPOS-00126, SRG-OS-000327-GPOS-00127

Audit:

Verify the operating system audits the execution of privileged functions.

Check if the operating system is configured to audit the execution of the "execve" system call, by running the following command:

```
# grep execve /etc/audit/audit.rules  
  
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -k execpriv  
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -k execpriv  
  
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -k execpriv  
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -k execpriv
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the operating system to audit the execution of the "execve" system call.
Add or update the following file system rules to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -k execpriv  
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -k execpriv  
  
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -k execpriv  
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -k execpriv
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230386

Rule ID: SV-230386r627750_rule

STIG ID: RHEL-08-030000

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.38 Ensure the operating system's audit daemon is configured to include local events (Automated)

Profile Applicability:

- STIG

Description:

The audit system must audit local events.

Rationale:

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Audit:

Verify the the operating system's audit daemon is configured to include local events, with the following command:

```
# grep local_events /etc/audit/auditd.conf  
local_events = yes
```

If the value of the "local_events" option is not set to "yes", or the line is commented out, this is a finding.

Remediation:

Configure the operating system to audit local events on the system.
Add or update the following line in "/etc/audit/auditd.conf" file:

```
local_events = yes
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230393

Rule ID: SV-230393r627750_rule

STIG ID: RHEL-08-030061

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.39 Ensure the operating system's audit daemon is configured to label all off-loaded audit logs (Automated)

Profile Applicability:

- STIG

Description:

The operating system must label all off-loaded audit logs before sending them to the central log server.

Rationale:

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Enriched logging is needed to determine who, what, and when events occur on a system. Without this, determining root cause of an event will be much more difficult. When audit logs are not labeled before they are sent to a central log server, the audit data will not be able to be analyzed and tied back to the correct system.

Audit:

Verify the operating system's audit daemon is configured to label all off-loaded audit logs, with the following command:

```
# grep "name_format" /etc/audit/auditd.conf  
name_format = hostname
```

If the "name_format" option is not "hostname", "fqdn", or "numeric", or the line is commented out, this is a finding.

Remediation:

Edit the /etc/audit/auditd.conf file and add or update the "name_format" option:

```
name_format = hostname
```

The audit daemon must be restarted for changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230394

Rule ID: SV-230394r627750_rule

STIG ID: RHEL-08-030062

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.6 Deploy SIEM or Log Analytic tool Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	●	●	

4.1.40 Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk (Automated)

Profile Applicability:

- STIG

Description:

The operating system must resolve audit information before writing to disk.

Rationale:

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Enriched logging aids in making sense of who, what, and when events occur on a system. Without this, determining root cause of an event will be much more difficult.

Audit:

Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk, with the following command:

```
# grep "log_format" /etc/audit/auditd.conf  
log_format = ENRICHED
```

If the "log_format" option is not "ENRICHED", or the line is commented out, this is a finding.

Remediation:

Edit the /etc/audit/auditd.conf file and add or update the "log_format" option:

```
log_format = ENRICHED
```

The audit daemon must be restarted for changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230395

Rule ID: SV-230395r627750_rule

STIG ID: RHEL-08-030063

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.41 Ensure the operating system's audit logs have a mode of "0600" or less permissive (Automated)

Profile Applicability:

- STIG

Description:

The operating system's audit logs must have a mode of 0600 or less permissive to prevent unauthorized read access.

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000206-GPOS-00084

Audit:

Verify the audit logs have a mode of "0600" or less permissive.

First, determine where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
log_file = /var/log/audit/audit.log
```

Using the location of the audit log file, check if the audit log has a mode of "0600" or less permissive with the following command:

```
# stat -c "%a %n" /var/log/audit/audit.log  
600 /var/log/audit/audit.log
```

If the audit log has a mode more permissive than "0600", this is a finding.

Remediation:

Configure the audit log to be protected from unauthorized read access by configuring the log group in the /etc/audit/auditd.conf file:

```
log_group = root
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230396

Rule ID: SV-230396r627750_rule

STIG ID: RHEL-08-030070

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.42 Ensure the operating system's audit logs are owned by "root" (Automated)

Profile Applicability:

- STIG

Description:

The operating system's audit logs must be owned by root to prevent unauthorized read access.

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000206-GPOS-00084

Audit:

Verify the audit logs are owned by "root". First, determine where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
log_file = /var/log/audit/audit.log
```

Using the location of the audit log file, determine if the audit log is owned by "root" using the following command:

```
# ls -al /var/log/audit/audit.log  
rw----- 2 root root 23 Jun 11 11:56 /var/log/audit/audit.log
```

If the audit log is not owned by "root", this is a finding.

Remediation:

Configure the audit log to be protected from unauthorized read access, by setting the correct owner as "root" with the following command:

```
# chown root [audit_log_file]
```

Replace "[audit_log_file]" to the correct audit log path, by default this location is "/var/log/audit/audit.log".

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230397

Rule ID: SV-230397r627750_rule

STIG ID: RHEL-08-030080

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.43 Ensure the audit logs are group-owned by "root" (Automated)

Profile Applicability:

- STIG

Description:

The operating system's audit logs must be group-owned by root to prevent unauthorized read access.

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit the operating system's activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit logs are group-owned by "root". First determine where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
log_file = /var/log/audit/audit.log
```

Using the location of the audit log file, determine if the audit log is group-owned by "root" using the following command:

```
ls -al /var/log/audit/audit.log  
rw----- 2 root root 23 Jun 11 11:56 /var/log/audit/audit.log
```

If the audit log is not group-owned by "root", this is a finding.

Remediation:

Configure the audit log to be owned by root by configuring the log group in the /etc/audit/auditd.conf file:

```
log_group = root
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230398

Rule ID: SV-230398r627750_rule

STIG ID: RHEL-08-030090

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.44 Ensure the audit log directory is owned by "root" to prevent unauthorized read access (Automated)

Profile Applicability:

- STIG

Description:

The audit log directory must be owned by root to prevent unauthorized read access.

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit the operating system's activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit log directory is owned by "root" to prevent unauthorized read access. Determine where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
log_file = /var/log/audit/audit.log
```

Determine the owner of the audit log directory by using the output of the above command (ex: "/var/log/audit/"). Run the following command with the correct audit log directory path:

```
# ls -ld /var/log/audit  
drw----- 2 root root 23 Jun 11 11:56 /var/log/audit
```

If the audit log directory is not owned by "root", this is a finding.

Remediation:

Configure the audit log to be protected from unauthorized read access, by setting the correct owner as "root" with the following command:

```
# chown root [audit_log_directory]
```

Replace "[audit_log_directory]" with the correct audit log directory path, by default this location is usually "/var/log/audit".

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230399

Rule ID: SV-230399r627750_rule

STIG ID: RHEL-08-030100

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.45 Ensure the audit log directory is group-owned by "root" to prevent unauthorized read access (Automated)

Profile Applicability:

- STIG

Description:

The operating system's audit log directory must be group-owned by root to prevent unauthorized read access.

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit the operating system's activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit log directory is group-owned by "root" to prevent unauthorized read access.

Determine where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
log_file = /var/log/audit/audit.log
```

Determine the group owner of the audit log directory by using the output of the above command (ex: "/var/log/audit/"). Run the following command with the correct audit log directory path:

```
# ls -ld /var/log/audit  
drw----- 2 root root 23 Jun 11 11:56 /var/log/audit  
` `` `  
  
If the audit log directory is not group-owned by "root", this is a finding.
```

Remediation:

Configure the audit log to be protected from unauthorized read access by setting the correct group-owner as "root" with the following command:

```
# chgrp root [audit_log_directory]
```

Replace "[audit_log_directory]" with the correct audit log directory path, by default this location is usually "/var/log/audit".

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230400

Rule ID: SV-230400r627750_rule

STIG ID: RHEL-08-030110

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.46 Ensure the audit log directories have a mode of "0700" or less permissive by first determining where the audit logs are stored (Automated)

Profile Applicability:

- STIG

Description:

The audit log directory must have a mode of 0700 or less permissive to prevent unauthorized read access.

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit log directories have a mode of "0700" or less permissive by first determining where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
log_file = /var/log/audit/audit.log
```

Using the location of the audit log, determine the directory where the audit logs are stored (ex: "/var/log/audit"). Run the following command to determine the permissions for the audit log folder:

```
# stat -c "%a %n" /var/log/audit  
700 /var/log/audit
```

If the audit log directory has a mode more permissive than "0700", this is a finding.

Remediation:

Configure the audit log directory to be protected from unauthorized read access by setting the correct permissive mode with the following command:

```
# chmod 0700 [audit_log_directory]
```

Replace "[audit_log_directory]" to the correct audit log directory path, by default this location is "/var/log/audit".

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230401

Rule ID: SV-230401r627750_rule

STIG ID: RHEL-08-030120

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.47 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chcon" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the chcon command in RHEL 8 must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chcon" command is used to change file SELinux security context.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "chcon" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w chcon /etc/audit/audit.rules
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset
-k perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chcon" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset  
-k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230419

Rule ID: SV-230419r627750_rule

STIG ID: RHEL-08-030260

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.48 Ensure the operating system is configured to audit the execution of the "setxattr" system call (Automated)

Profile Applicability:

- STIG

Description:

The audit system must be configured to audit any usage of the setxattr system call.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). "Setxattr" is a system call used to set an extended attribute value.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify if the operating system is configured to audit the execution of the "setxattr" system call, by running the following command:

```
# grep -w setxattr /etc/audit/audit.rules

-a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=unset -k
perm_mod
-a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=unset -k
perm_mod

-a always,exit -F arch=b32 -S setxattr -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -F auid=0 -k perm_mod
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the operating system to audit the execution of the "setxattr" system call, by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=unset -k perm_mod  
-a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=unset -k perm_mod  
  
-a always,exit -F arch=b32 -S setxattr -F auid=0 -k perm_mod  
-a always,exit -F arch=b64 -S setxattr -F auid=0 -k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230420

Rule ID: SV-230420r627750_rule

STIG ID: RHEL-08-030270

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.49 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
# grep /etc/passwd /etc/audit/audit.rules  
-w /etc/passwd -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/passwd -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230406

Rule ID: SV-230406r627750_rule

STIG ID: RHEL-08-030150

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.50 Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, CCI-002884, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
# grep /etc/group /etc/audit/audit.rules  
-w /etc/group -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/group -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230408

Rule ID: SV-230408r627750_rule

STIG ID: RHEL-08-030170

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.51 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-agent" (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the ssh-agent must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "ssh-agent" is a program to hold private keys used for public key authentication.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "ssh-agent" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep ssh-agent /etc/audit/audit.rules
-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-ssh
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "ssh-agent" by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-ssh
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230421

Rule ID: SV-230421r627750_rule

STIG ID: RHEL-08-030280

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.52 Ensure an audit event is generated for any successful/unsuccessful use of the "passwd" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the passwd command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "passwd" command is used to change passwords for user accounts.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "passwd" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w passwd /etc/audit/audit.rules
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-passwd
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "passwd" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230422

Rule ID: SV-230422r627750_rule

STIG ID: RHEL-08-030290

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.53 Ensure an audit event is generated for any successful/unsuccessful use of the "mount" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the mount command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "mount" command is used to mount a filesystem.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "mount" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w /usr/bin/mount /etc/audit/audit.rules
-a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-mount
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "mount" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-mount
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230423

Rule ID: SV-230423r627750_rule

STIG ID: RHEL-08-030300

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.54 Ensure an audit event is generated for any successful/unsuccessful use of the "umount" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the umount command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "umount" command is used to unmount a filesystem.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "umount" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w /usr/bin/umount /etc/audit/audit.rules
-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-mount
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "umount" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-mount
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230424

Rule ID: SV-230424r627750_rule

STIG ID: RHEL-08-030301

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.55 Ensure an audit event is generated for any successful/unsuccessful use of the "mount" syscall (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the mount syscall must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "mount" syscall is used to mount a filesystem.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "mount" syscall by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "\-S mount" /etc/audit/audit.rules
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -k
privileged-mount
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -k
privileged-mount
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "mount" syscall by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -k  
privileged-mount  
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -k  
privileged-mount
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230425

Rule ID: SV-230425r627750_rule

STIG ID: RHEL-08-030302

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.56 Ensure an audit event is generated for any successful/unsuccessful use of the "unix_update" (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the unix_update must generate an audit record.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. "Unix_update" is a helper program for the "pam_unix" module that updates the password for a given user. It is not intended to be run directly from the command line and logs a security violation if done so.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "unix_update" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "unix_update" /etc/audit/audit.rules  
-a always,exit -F path=/usr/sbin/unix_update -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "unix_update" by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/unix_update -F perm=x -F auid>=1000 -F auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230426

Rule ID: SV-230426r627750_rule

STIG ID: RHEL-08-030310

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.57 Ensure an audit event is generated for any successful/unsuccessful use of "postdrop" (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of postdrop must generate an audit record.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "postdrop" command creates a file in the maildrop directory and copies its standard input to the file.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of "postdrop" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "postdrop" /etc/audit/audit.rules
-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "postdrop" by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230427

Rule ID: SV-230427r627750_rule

STIG ID: RHEL-08-030311

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.58 Ensure an audit event is generated for any successful/unsuccessful use of "postqueue" (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of postqueue must generate an audit record.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "postqueue" command implements the Postfix user interface for queue management.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of "postqueue" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "postqueue" /etc/audit/audit.rules
-a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "postqueue" by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230428

Rule ID: SV-230428r627750_rule

STIG ID: RHEL-08-030312

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.59 Ensure an audit event is generated for any successful/unsuccessful use of "semanage" (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of semanage must generate an audit record.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "semanage" command is used to configure certain elements of SELinux policy without requiring modification to or recompilation from policy sources.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of "semanage" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "semanage" /etc/audit/audit.rules
-a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "semanage" by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230429

Rule ID: SV-230429r627750_rule

STIG ID: RHEL-08-030313

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.60 Ensure an audit event is generated for any successful/unsuccessful use of "setfiles" (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of setfiles must generate an audit record.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "setfiles" command is primarily used to initialize the security context fields (extended attributes) on one or more filesystems (or parts of them). Usually it is initially run as part of the SELinux installation process (a step commonly known as labeling).

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of "setfiles" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "setfiles" /etc/audit/audit.rules
-a always,exit -F path=/usr/sbin/setfiles -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "setfiles" by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/setfiles -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230430

Rule ID: SV-230430r627750_rule

STIG ID: RHEL-08-030314

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.61 Ensure an audit event is generated for any successful/unsuccessful use of "userhelper" (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of userhelper must generate an audit record.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "userhelper" command is not intended to be run interactively. "Userhelper" provides a basic interface to change a user's password, gecos information, and shell. The main difference between this program and its traditional equivalents (passwd, chfn, chsh) is that prompts are written to standard out to make it easy for a graphical user interface wrapper to interface to it as a child process.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of "userhelper" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "userhelper" /etc/audit/audit.rules
-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "userhelper" by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230431

Rule ID: SV-230431r627750_rule

STIG ID: RHEL-08-030315

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.62 Ensure an audit event is generated for any successful/unsuccessful use of "setsebool" (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of setsebool must generate an audit record.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "setsebool" command sets the current state of a particular SELinux boolean or a list of booleans to a given value.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of "setsebool" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "setsebool" /etc/audit/audit.rules
-a always,exit -F path=/usr/sbin/setsebool -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "setsebool" by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/setsebool -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230432

Rule ID: SV-230432r627750_rule

STIG ID: RHEL-08-030316

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.63 Ensure an audit event is generated for any successful/unsuccessful use of "unix_chkpwd" (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of unix_chkpwd must generate an audit record.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "unix_chkpwd" command is a helper program for the pam_unix module that verifies the password of the current user. It also checks password and account expiration dates in shadow. It is not intended to be run directly from the command line and logs a security violation if done so.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of "unix_chkpwd" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "unix_chkpwd" /etc/audit/audit.rules
-a always,exit -F path=/usr/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "unix_chkpwd" by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230433

Rule ID: SV-230433r627750_rule

STIG ID: RHEL-08-030317

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.64 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-keysign" (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the ssh-keysign must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "ssh-keysign" program is an SSH helper program for host-based authentication.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "ssh-keysign" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep ssh-keysign /etc/audit/audit.rules  
-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F  
auid>=1000 -F auid!=unset -k privileged-ssh
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "ssh-keysign" by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/libexec.openssh/ssh-keysign -F perm=x -F auid>=1000 -F auid!=unset -k privileged-ssh
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230434

Rule ID: SV-230434r744002_rule

STIG ID: RHEL-08-030320

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.65 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "setfacl" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the setfacl command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "setfacl" command is used to set file access control lists.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "setfacl" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w setfacl /etc/audit/audit.rules
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=unset -k perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "setfacl" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F  
auid!=unset -k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230435

Rule ID: SV-230435r627750_rule

STIG ID: RHEL-08-030330

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.66 Ensure an audit event is generated for any successful/unsuccessful use of the "pam_timestamp_check" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the pam_timestamp_check command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "pam_timestamp_check" command is used to check if the default timestamp is valid.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "pam_timestamp_check" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w pam_timestamp_check /etc/audit/audit.rules  
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000  
-F auid!=unset -k privileged-pam_timestamp_check
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "pam_timestamp_check" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000  
-F auid!=unset -k privileged-pam_timestamp_check
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230436

Rule ID: SV-230436r627750_rule

STIG ID: RHEL-08-030340

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.67 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "newgrp" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the newgrp command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "newgrp" command is used to change the current group ID during a login session.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "newgrp" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w newgrp /etc/audit/audit.rules
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=unset
-k priv_cmd
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "newgrp" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=unset  
-k priv_cmd
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230437

Rule ID: SV-230437r627750_rule

STIG ID: RHEL-08-030350

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.68 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "init_module" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the init_module command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "init_module" command is used to load a kernel module.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "init_module" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "init_module" /etc/audit/audit.rules
-a always,exit -F arch=b32 -S init_module -F auid>=1000 -F auid!=unset -k
module_chng
-a always,exit -F arch=b64 -S init_module -F auid>=1000 -F auid!=unset -k
module_chng
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "init_module" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S init_module -F auid>=1000 -F auid!=unset -k module_chng  
-a always,exit -F arch=b64 -S init_module -F auid>=1000 -F auid!=unset -k module_chng
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230438

Rule ID: SV-230438r627750_rule

STIG ID: RHEL-08-030360

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.69 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rename" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the rename command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "rename" command will rename the specified files by replacing the first occurrence of expression in their name by replacement.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "rename" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "rename" /etc/audit/audit.rules
-a always,exit -F arch=b32 -S rename -F auid>=1000 -F auid!=unset -k delete
-a always,exit -F arch=b64 -S rename -F auid>=1000 -F auid!=unset -k delete
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "rename" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S rename -F auid>=1000 -F auid!=unset -k delete  
-a always,exit -F arch=b64 -S rename -F auid>=1000 -F auid!=unset -k delete
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230439

Rule ID: SV-230439r627750_rule

STIG ID: RHEL-08-030361

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.70 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "renameat" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the renameat command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "renameat" command renames a file, moving it between directories if required.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "renameat" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "renameat" /etc/audit/audit.rules
-a always,exit -F arch=b32 -S renameat -F auid>=1000 -F auid!=unset -k delete
-a always,exit -F arch=b64 -S renameat -F auid>=1000 -F auid!=unset -k delete
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "renameat" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S renameat -F auid>=1000 -F auid!=unset -k delete  
-a always,exit -F arch=b64 -S renameat -F auid>=1000 -F auid!=unset -k delete
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230440

Rule ID: SV-230440r627750_rule

STIG ID: RHEL-08-030362

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.71 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rmdir" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the rmdir command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "rmdir" command removes empty directories.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "rmdir" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "rmdir" /etc/audit/audit.rules
-a always,exit -F arch=b32 -S rmdir -F auid>=1000 -F auid!=unset -k delete
-a always,exit -F arch=b64 -S rmdir -F auid>=1000 -F auid!=unset -k delete
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "rmdir" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S rmdir -F auid>=1000 -F auid!=unset -k delete  
-a always,exit -F arch=b64 -S rmdir -F auid>=1000 -F auid!=unset -k delete
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230441

Rule ID: SV-230441r627750_rule

STIG ID: RHEL-08-030363

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.72 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlink" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the unlink command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "unlink" command deletes a name from the filesystem. If that name was the last link to a file and no processes have the file open, the file is deleted and the space it was using is made available for reuse.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "unlink" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "unlink" /etc/audit/audit.rules
-a always,exit -F arch=b32 -S unlink -F auid>=1000 -F auid!=unset -k delete
-a always,exit -F arch=b64 -S unlink -F auid>=1000 -F auid!=unset -k delete
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "unlink" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S unlink -F auid>=1000 -F auid!=unset -k delete  
-a always,exit -F arch=b64 -S unlink -F auid>=1000 -F auid!=unset -k delete
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230442

Rule ID: SV-230442r627750_rule

STIG ID: RHEL-08-030364

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.73 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlinkat" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the unlinkat command in RHEL 8 must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "unlinkat" system call operates in exactly the same way as either "unlink" or "rmdir" except for the differences described in the manual page.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "unlinkat" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "unlinkat" /etc/audit/audit.rules
-a always,exit -F arch=b32 -S unlinkat -F auid>=1000 -F auid!=unset -k delete
-a always,exit -F arch=b64 -S unlinkat -F auid>=1000 -F auid!=unset -k delete
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "unlink" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S unlinkat -F auid>=1000 -F auid!=unset -k delete  
-a always,exit -F arch=b64 -S unlinkat -F auid>=1000 -F auid!=unset -k delete
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230443

Rule ID: SV-230443r627750_rule

STIG ID: RHEL-08-030365

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.74 Ensure an audit event is generated for any successful/unsuccessful use of the "gpasswd" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the gpasswd command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "gpasswd" command is used to administer /etc/group and /etc/gshadow. Every group can have administrators, members and a password.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "gpasswd" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w gpasswd /etc/audit/audit.rules  
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-gpasswd
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "gpasswd" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-gpasswd
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230444

Rule ID: SV-230444r627750_rule

STIG ID: RHEL-08-030370

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.75 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "finit_module" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the finit_module command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "finit_module" command is used to load a kernel module.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "finit_module" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "finit_module" /etc/audit/audit.rules
-a always,exit -F arch=b32 -S finit_module -F auid>=1000 -F auid!=unset -k
module_chng
-a always,exit -F arch=b64 -S finit_module -F auid>=1000 -F auid!=unset -k
module_chng
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "finit_module" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S finit_module -F auid>=1000 -F auid!=unset -k module_chng  
-a always,exit -F arch=b64 -S finit_module -F auid>=1000 -F auid!=unset -k module_chng
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230445

Rule ID: SV-230445r627750_rule

STIG ID: RHEL-08-030380

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.76 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "delete_module" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the delete_module command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "delete_module" command is used to unload a kernel module.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "delete_module" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "delete_module" /etc/audit/audit.rules
-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=unset -k
module_chng
-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=unset -k
module_chng
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "delete_module" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=unset -k module_chng  
-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=unset -k module_chng
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230446

Rule ID: SV-230446r627750_rule

STIG ID: RHEL-08-030390

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.77 Ensure an audit event is generated for any successful/unsuccessful use of the "crontab" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the crontab command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "crontab" command is used to maintain crontab files for individual users. Crontab is the program used to install, remove, or list the tables used to drive the cron daemon. This is similar to the task scheduler used in other operating systems.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "crontab" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w crontab /etc/audit/audit.rules
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-crontab
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "crontab" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-crontab
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230447

Rule ID: SV-230447r627750_rule

STIG ID: RHEL-08-030400

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.78 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chsh" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the chsh command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chsh" command is used to change the login shell.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "chsh" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w chsh /etc/audit/audit.rules
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=unset -
k priv_cmd
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chsh" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=unset -k priv_cmd
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230448

Rule ID: SV-230448r627750_rule

STIG ID: RHEL-08-030410

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.79 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "truncate" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the truncate command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "truncate" and "ftruncate" functions are used to truncate a file to a specified length.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "truncate" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -iw truncate /etc/audit/audit.rules

-a always,exit -F arch=b32 -S truncate -F exit==EPERM -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S truncate -F exit==EPERM -F auid>=1000 -F
auid!=unset -k perm_access

-a always,exit -F arch=b32 -S truncate -F exit==EACCES -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S truncate -F exit==EACCES -F auid>=1000 -F
auid!=unset -k perm_access
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "truncate" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S truncate -F exit==EPERM -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S truncate -F exit==EPERM -F auid>=1000 -F
auid!=unset -k perm_access

-a always,exit -F arch=b32 -S truncate -F exit==EACCES -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S truncate -F exit==EACCES -F auid>=1000 -F
auid!=unset -k perm_access
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230449

Rule ID: SV-230449r627750_rule

STIG ID: RHEL-08-030420

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.80 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "openat" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the openat system call in the operating system must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "openat" system call opens a file specified by a relative pathname.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "openat" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -iw openat /etc/audit/audit.rules

-a always,exit -F arch=b32 -S openat -F exit=-EPERM -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S openat -F exit=-EPERM -F auid>=1000 -F
auid!=unset -k perm_access

-a always,exit -F arch=b32 -S openat -F exit=-EACCES -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S openat -F exit=-EACCES -F auid>=1000 -F
auid!=unset -k perm_access
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "openat" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S openat -F exit=-EPERM -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S openat -F exit=-EPERM -F auid>=1000 -F
auid!=unset -k perm_access

-a always,exit -F arch=b32 -S openat -F exit=-EACCES -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S openat -F exit=-EACCES -F auid>=1000 -F
auid!=unset -k perm_access
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230450

Rule ID: SV-230450r627750_rule

STIG ID: RHEL-08-030430

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.81 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open" system call (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the open system call must generate an audit record.

Rationale:

Successful/unsuccessful uses of the open system call in RHEL 8 must generate an audit record.

Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "open system" call opens a file specified by a pathname. If the specified file does not exist, it may optionally be created by "open".

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "open" system call by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -iw open /etc/audit/audit.rules

-a always,exit -F arch=b32 -S open -F exit=-EPERM -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S open -F exit=-EPERM -F auid>=1000 -F
auid!=unset -k perm_access

-a always,exit -F arch=b32 -S open -F exit=-EACCES -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S open -F exit=-EACCES -F auid>=1000 -F
auid!=unset -k perm_access
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "open" system call by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S open -F exit=-EPERM -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S open -F exit=-EPERM -F auid>=1000 -F
auid!=unset -k perm_access

-a always,exit -F arch=b32 -S open -F exit=-EACCES -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S open -F exit=-EACCES -F auid>=1000 -F
auid!=unset -k perm_access
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230451

Rule ID: SV-230451r627750_rule

STIG ID: RHEL-08-030440

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.82 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open_by_handle_at" system call (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the open_by_handle_at system call must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "name_to_handle_at" and "open_by_handle_at" system calls split the functionality of openat into two parts: "name_to_handle_at" returns an opaque handle that corresponds to a specified file; "open_by_handle_at" opens the file corresponding to a handle returned by a previous call to "name_to_handle_at" and returns an open file descriptor.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "open_by_handle_at" system call by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -iw open_by_handle_at /etc/audit/audit.rules

-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EPERM -F auid>=1000
-F auid!=unset -k perm_access
-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EPERM -F auid>=1000
-F auid!=unset -k perm_access

-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EACCES -F auid>=1000
-F auid!=unset -k perm_access
-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EACCES -F auid>=1000
-F auid!=unset -k perm_access
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "open_by_handle_at" system call by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EPERM -F auid>=1000
-F auid!=unset -k perm_access
-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EPERM -F auid>=1000
-F auid!=unset -k perm_access

-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EACCES -F auid>=1000
-F auid!=unset -k perm_access
-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EACCES -F auid>=1000
-F auid!=unset -k perm_access
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230452

Rule ID: SV-230452r627750_rule

STIG ID: RHEL-08-030450

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.83 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ftruncate" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the ftruncate command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "truncate" and "ftruncate" functions are used to truncate a file to a specified length.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "ftruncate" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -iw ftruncate /etc/audit/audit.rules

-a always,exit -F arch=b32 -S ftruncate -F exit==EPERM -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S ftruncate -F exit==EPERM -F auid>=1000 -F
auid!=unset -k perm_access

-a always,exit -F arch=b32 -S ftruncate -F exit==EACCES -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S ftruncate -F exit==EACCES -F auid>=1000 -F
auid!=unset -k perm_access
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "ftruncate" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S ftruncate -F exit==EPERM -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S ftruncate -F exit==EPERM -F auid>=1000 -F
auid!=unset -k perm_access

-a always,exit -F arch=b32 -S ftruncate -F exit==EACCES -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S ftruncate -F exit==EACCES -F auid>=1000 -F
auid!=unset -k perm_access
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230453

Rule ID: SV-230453r627750_rule

STIG ID: RHEL-08-030460

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.84 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "creat" system call (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the creat system call must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "creat" system call is used to open and possibly create a file or device.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "creat" system call by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -iw creat /etc/audit/audit.rules

-a always,exit -F arch=b32 -S creat -F exit=-EPERM -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S creat -F exit=-EPERM -F auid>=1000 -F
auid!=unset -k perm_access

-a always,exit -F arch=b32 -S creat -F exit=-EACCES -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S creat -F exit=-EACCES -F auid>=1000 -F
auid!=unset -k perm_access
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "creat" system call by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S creat -F exit=-EPERM -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S creat -F exit=-EPERM -F auid>=1000 -F
auid!=unset -k perm_access

-a always,exit -F arch=b32 -S creat -F exit=-EACCES -F auid>=1000 -F
auid!=unset -k perm_access
-a always,exit -F arch=b64 -S creat -F exit=-EACCES -F auid>=1000 -F
auid!=unset -k perm_access
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230454

Rule ID: SV-230454r627750_rule

STIG ID: RHEL-08-030470

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.85 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chown" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the chown command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chown" command is used to change file owner and group.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "chown" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w chown /etc/audit/audit.rules
-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=unset -k perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chown" command by adding or updating the following line to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=unset -k perm_mod  
-a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=unset -k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230455

Rule ID: SV-230455r627750_rule

STIG ID: RHEL-08-030480

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.86 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chmod" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the chmod command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chmod" command changes the file mode bits of each given file according to mode, which can be either a symbolic representation of changes to make, or an octal number representing the bit pattern for the new mode bits.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210

Audit:

Ensure the operating system generates an audit record when successful/unsuccessful attempts to use the "chmod" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w chmod /etc/audit/audit.rules
-a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=unset -k perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chmod" command by adding or updating the following line to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=unset -k perm_mod  
-a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=unset -k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230456

Rule ID: SV-230456r627750_rule

STIG ID: RHEL-08-030490

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.87 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "lchown" system call (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the lchown system call must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "lchown" system call is used to change the ownership of the file specified by a path, which does not dereference symbolic links.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "lchown" system call by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w lchown /etc/audit/audit.rules
-a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=unset -k perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "lchown" system call by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=unset -k perm_mod  
-a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=unset -k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230457

Rule ID: SV-230457r627750_rule

STIG ID: RHEL-08-030500

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.88 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchownat" system call (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the fchownat system call must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "fchownat" system call is used to change the ownership of a file referred to by the open file descriptor.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "fchownat" system call by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w fchownat /etc/audit/audit.rules
-a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=unset -k
perm_mod
-a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=unset -k
perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "fchownat" system call by adding or updating the following line to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=unset -k  
perm_mod  
-a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=unset -k  
perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230458

Rule ID: SV-230458r627750_rule

STIG ID: RHEL-08-030510

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.89 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchown" system call (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the fchown system call must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "fchown" system call is used to change the ownership of a file referred to by the open file descriptor.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "fchown" system call by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w fchown /etc/audit/audit.rules
-a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=unset -k perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "fchown" system call by adding or updating the following line to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=unset -k perm_mod  
-a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=unset -k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230459

Rule ID: SV-230459r627750_rule

STIG ID: RHEL-08-030520

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.90 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmod" system call (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the fchmod system call must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "fchmod" system call is used to change permissions of a file.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "fchmod" system call by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w fchmod /etc/audit/audit.rules
-a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=unset -k perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "fchmod" system call by adding or updating the following line to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=unset -k perm_mod  
-a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=unset -k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230461

Rule ID: SV-230461r627750_rule

STIG ID: RHEL-08-030540

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.91 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmodat" system call (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the fchmodat system call must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "fchmodat" system call is used to change permissions of a file relative to a directory file descriptor.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "fchmodat" system call by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w fchmodat /etc/audit/audit.rules
-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=unset -k
perm_mod
-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=unset -k
perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "fchmodat" system call by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=unset -k  
perm_mod  
-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=unset -k  
perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230460

Rule ID: SV-230460r627750_rule

STIG ID: RHEL-08-030530

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.92 Ensure an audit event is generated for any successful/unsuccessful use of the "sudo" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the sudo command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "sudo" command allows a permitted user to execute a command as the superuser or another user, as specified by the security policy.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "sudo" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w sudo /etc/audit/audit.rules
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=unset -
k priv_cmd
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "sudo" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=unset -k priv_cmd
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230462

Rule ID: SV-230462r627750_rule

STIG ID: RHEL-08-030550

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.			

4.1.93 Ensure an audit event is generated for any successful/unsuccessful use of the "usermod" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the usermod command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "usermod" command modifies the system account files to reflect the changes that are specified on the command line.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "usermod" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w usermod /etc/audit/audit.rules
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-usermod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "usermod" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-usermod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230463

Rule ID: SV-230463r627750_rule

STIG ID: RHEL-08-030560

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.94 Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chacl" command (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the chacl command must generate an audit record.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chacl" command is used to change the access control list of a file or directory.

When a user logs on, the AUID is set to the UID of the account that is being authenticated.

Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210

Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "chacl" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w chacl /etc/audit/audit.rules
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=unset
-k perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chacl" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=unset  
-k perm_mod
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230464

Rule ID: SV-230464r627750_rule

STIG ID: RHEL-08-030570

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.95 Ensure the operating system is configured to audit the execution of the module management program "kmod" (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful uses of the kmod command must generate an audit record.

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one. Audit records can be generated from various components within the information system (e.g., module or policy filter). The "kmod" command is used to control Linux Kernel modules.

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the list of events for which the operating system will provide an audit record generation capability as the following:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Verify if the operating system is configured to audit the execution of the module management program "kmod", by running the following command:

```
# grep "/usr/bin/kmod" /etc/audit/audit.rules  
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -  
k modules
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to audit the execution of the module management program "kmod" by adding or updating the following line to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -  
k modules
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230465

Rule ID: SV-230465r627750_rule

STIG ID: RHEL-08-030580

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.96 Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "faillock" file occur (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful modifications to the faillock log file must generate an audit record.

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one. Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the list of events for which the operating system will provide an audit record generation capability as the following:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

From "Pam_Faillock man" pages: Note the default directory that pam_faillock uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218

Audit:

Verify the operating system generates an audit record when successful/unsuccessful modifications to the "faillock" file occur. First, determine where the faillock tallies are stored with the following commands:

For RHEL versions 8.0 and 8.1:

```
# grep -i pam_faillock.so /etc/pam.d/system-auth  
  
auth required pam_faillock.so preauth dir=/var/log/faillock silent deny=3  
fail_interval=900 even_deny_root
```

For RHEL versions 8.2 and newer:

```
# grep dir /etc/security/faillock.conf  
  
dir=/var/log/faillock
```

Using the location of the faillock log file, check that the following calls are being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w faillock /etc/audit/audit.rules  
  
-w /var/log/faillock -p wa -k logins
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful modifications to the "faillock" file by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-w /var/log/faillock -p wa -k logins
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230466

Rule ID: SV-230466r627750_rule

STIG ID: RHEL-08-030590

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.97 Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "lastlog" file (Automated)

Profile Applicability:

- STIG

Description:

Successful/unsuccessful modifications to the lastlog file must generate an audit record.

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one. Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the list of events for which the operating system will provide an audit record generation capability as the following:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218

Audit:

Verify the operating system generates an audit record when successful/unsuccessful modifications to the "lastlog" file by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w lastlog /etc/audit/audit.rules  
-w /var/log/lastlog -p wa -k logins
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful modifications to the "lastlog" file by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-w /var/log/lastlog -p wa -k logins
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230467

Rule ID: SV-230467r627750_rule

STIG ID: RHEL-08-030600

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.98 Ensure the operating system enables auditing of processes that start prior to the audit daemon (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enable auditing of processes that start prior to the audit daemon.

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one. If auditing is enabled late in the startup process, the actions of some startup processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the list of events for which RHEL 8 will provide an audit record generation capability as the following:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218

Audit:

Verify the operating system enables auditing of processes that start prior to the audit daemon with the following commands:

```
# grub2-editenv - list | grep audit  
  
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto  
resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb  
quiet fips=1 audit=1 audit_backlog_limit=8192 boot=UUID=8d171156-cd61-421c-  
ba41-1c021ac29e82
```

If the "audit" entry does not equal "1", is missing, or the line is commented out, this is a finding.

Check that auditing is enabled by default to persist in kernel updates:

```
# grep audit /etc/default/grub  
  
GRUB_CMDLINE_LINUX="audit=1"
```

If "audit" is not set to "1", is missing or commented out, this is a finding.

Remediation:

Configure the operating system to audit processes that start prior to the audit daemon with the following command:

```
# grubby --update-kernel=ALL --args="audit=1"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="audit=1"
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230468

Rule ID: SV-230468r627750_rule

STIG ID: RHEL-08-030601

Severity: CAT

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.99 Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon (Automated)

Profile Applicability:

- STIG

Description:

The operating system must allocate an audit_backlog_limit of sufficient size to capture processes that start prior to the audit daemon.

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one. If auditing is enabled late in the startup process, the actions of some startup processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Allocating an audit_backlog_limit of sufficient size is critical in maintaining a stable boot process. With an insufficient limit allocated, the system is susceptible to boot failures and crashes.

Audit:

Verify the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon with the following commands:

```
# grub2-editenv - list | grep audit  
  
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto  
resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb  
quiet fips=1 audit=1 audit_backlog_limit=8192 boot=UUID=8d171156-cd61-421c-  
ba41-1c021ac29e82
```

If the "audit_backlog_limit" entry does not equal "8192" or greater, is missing, or the line is commented out, this is a finding.

Check the audit_backlog_limit is set to persist in kernel updates:

```
# grep audit /etc/default/grub  
  
GRUB_CMDLINE_LINUX="audit_backlog_limit=8192"
```

If "audit_backlog_limit" is not set to "8192" or greater, is missing or commented out, this is a finding.

Remediation:

Configure the operating system to allocate sufficient audit_backlog_limit to capture processes that start prior to the audit daemon with the following command:

```
# grubby --update-kernel=ALL --args="audit_backlog_limit=8192"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="audit_backlog_limit=8192"
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230469

Rule ID: SV-230469r744004_rule

STIG ID: RHEL-08-030602

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.1.100 Ensure the operating system enables Linux audit logging of the USBGuard daemon (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enable Linux audit logging for the USBGuard daemon.

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one. If auditing is enabled late in the startup process, the actions of some startup processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the list of events for which the operating system will provide an audit record generation capability as the following:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system enables Linux audit logging of the USGuard daemon with the following commands:

Note: If the USGuard daemon is not installed and enabled, this requirement is not applicable.

```
# grep -i auditbackend /etc/usbguard/usbguard-daemon.conf  
AuditBackend=LinuxAudit
```

If the "AuditBackend" entry does not equal "LinuxAudit", is missing, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to enable Linux audit logging of the USGuard daemon by adding or modifying the following line in "/etc/usbguard/usbguard-daemon.conf":

```
AuditBackend=LinuxAudit
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230470

Rule ID: SV-230470r744006_rule

STIG ID: RHEL-08-030603

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.101 Ensure the files in directory "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive (Automated)

Profile Applicability:

- STIG

Description:

The operating system must allow only the Information System Security Manager (ISSM) (or individuals or roles appointed by the ISSM) to select which auditable events are to be audited.

Rationale:

Without the capability to restrict the roles and individuals that can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events.

Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit:

Verify that the files in directory "/etc/audit/rules.d/" and "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive by using the following commands:

```
# ls -al /etc/audit/rules.d/*.rules
-rw-r----- 1 root root 1280 Feb 16 17:09 audit.rules
# ls -l /etc/audit/auditd.conf
-rw-r----- 1 root root 621 Sep 22 17:19 auditd.conf
```

If the files in the "/etc/audit/rules.d/" directory or the "/etc/audit/auditd.conf" file have a mode more permissive than "0640", this is a finding.

Remediation:

Configure the files in directory "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file to have a mode of "0640" with the following commands:

```
# chmod 0640 /etc/audit/rules.d/audit.rules
# chmod 0640 /etc/audit/rules.d/[customrulesfile].rules
# chmod 0640 /etc/audit/auditd.conf
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230471

Rule ID: SV-230471r627750_rule

STIG ID: RHEL-08-030610

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.102 Ensure the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode (Automated)

Profile Applicability:

- STIG

Description:

The operating system's audit tools must have a mode of 0755 or less permissive.

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

RHEL 8 systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools, and the corresponding rights the user enjoys, to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Audit:

Verify the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode.

Check the octal permission of each audit tool by running the following command:

```
# stat -c "%a %n" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/rsyslogd /sbin/augenrules  
  
755 /sbin/auditctl  
755 /sbin/aureport  
755 /sbin/ausearch  
750 /sbin/autrace  
755 /sbin/auditd  
755 /sbin/rsyslogd  
755 /sbin/augenrules
```

If any of the audit tools has a mode more permissive than "0755", this is a finding.

Remediation:

Configure the audit tools to be protected from unauthorized access by setting the correct permissive mode using the following command:

```
# chmod 0755 [audit_tool]
```

Replace "[audit_tool]" with the audit tool that does not have the correct permissive mode.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230472

Rule ID: SV-230472r627750_rule

STIG ID: RHEL-08-030620

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.103 Ensure the audit tools are owned by "root" to prevent any unauthorized access, deletion, or modification (Automated)

Profile Applicability:

- STIG

Description:

The operating system's audit tools must be owned by root.

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

RHEL 8 systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools, and the corresponding rights the user enjoys, to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Satisfies: SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099

Audit:

Verify the audit tools are owned by "root" to prevent any unauthorized access, deletion, or modification.

Check the owner of each audit tool by running the following command:

```
# stat -c "%U %n" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/rsyslogd /sbin/augenrules  
  
root /sbin/auditctl  
root /sbin/aureport  
root /sbin/ausearch  
root /sbin/autrace  
root /sbin/auditd  
root /sbin/rsyslogd  
root /sbin/augenrules
```

If any of the audit tools are not owned by "root", this is a finding.

Remediation:

Configure the audit tools to be owned by "root", by running the following command:

```
# chown root [audit_tool]
```

Replace "[audit_tool]" with each audit tool not owned by "root".

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230473

Rule ID: SV-230473r744008_rule

STIG ID: RHEL-08-030630

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

4.1.104 Ensure the audit tools are group-owned by "root" to prevent any unauthorized access, deletion, or modification (Automated)

Profile Applicability:

- STIG

Description:

The operating system's audit tools must be group-owned by root.

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

RHEL 8 systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools, and the corresponding rights the user enjoys, to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Satisfies: SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099

Audit:

Verify the audit tools are group-owned by "root" to prevent any unauthorized access, deletion, or modification.

Check the owner of each audit tool by running the following commands:

```
# stat -c "%G %n" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/rsyslogd /sbin/augenrules  
  
root /sbin/auditctl  
root /sbin/aureport  
root /sbin/ausearch  
root /sbin/autrace  
root /sbin/auditd  
root /sbin/rsyslogd  
root /sbin/augenrules
```

If any of the audit tools are not group-owned by "root", this is a finding.

Remediation:

Configure the audit tools to be group-owned by "root", by running the following command:

```
# chgrp root [audit_tool]
```

Replace "[audit_tool]" with each audit tool not group-owned by "root".

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230474

Rule ID: SV-230474r627750_rule

STIG ID: RHEL-08-030640

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

4.1.105 Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent (Automated)

Profile Applicability:

- STIG

Description:

The operating system must notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when allocated audit record storage volume 75 percent utilization.

Rationale:

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Audit:

Verify the operating system notifies the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity with the following command:

```
# grep -w space_left_action /etc/audit/auditd.conf  
space_left_action = email
```

If the value of the "space_left_action" is not set to "email", or if the line is commented out, ask the System Administrator to indicate how the system is providing real-time alerts to the SA and ISSO.

If there is no evidence that real-time alerts are configured on the system, this is a finding.

Remediation:

Configure the operating system to initiate an action to notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity by adding/modifying the following line in the "/etc/audit/auditd.conf" file.

```
space_left_action = email
```

Note: Option names and values in the auditd.conf file are case insensitive.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244543

Rule ID: SV-244543r743878_rule

STIG ID: RHEL-08-030731

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.	●	●	

4.2 Configure Logging

Logging services should be configured to prevent information leaks and to aggregate logs on a remote server so that they can be reviewed in the event of a system compromise and ease log analysis.

4.2.1 Configure rsyslog

The `rsyslog` software is recommended as a replacement for the `syslogd` daemon and provides improvements over `syslogd`, such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

Note: This section only applies if `rsyslog` is installed on the system.

4.2.1.1 Ensure rsyslog is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsyslog` software is a recommended replacement to the original `syslogd` daemon which provide improvements over `syslogd`, such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

Rationale:

The security enhancements of `rsyslog` such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

Audit:

Verify rsyslog is installed.

Run the following command

```
# rpm -q rsyslog  
rsyslog-<version>
```

Remediation:

Run the following command to install rsyslog:

```
# dnf install rsyslog
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.2.1.2 Ensure the rsyslog service is enabled and active (Automated)

Profile Applicability:

- STIG

Description:

The rsyslog service must be running.

Rationale:

Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across the DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Audit:

Verify the rsyslog service is enabled and active with the following commands:

```
# systemctl is-enabled rsyslog  
enabled  
  
# systemctl is-active rsyslog  
active
```

If the service is not "enabled" and "active" this is a finding.

Remediation:

Start the auditd service, and enable the rsyslog service with the following commands:

```
# systemctl start rsyslog.service  
# systemctl enable rsyslog.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230298

Rule ID: SV-230298r627750_rule

STIG ID: RHEL-08-010561

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.2.1.3 Ensure the operating system monitors all remote access methods (Automated)

Profile Applicability:

- STIG

Description:

All operating system remote access methods must be monitored.

Rationale:

Remote access services, such as those providing remote access to network devices and information systems which lack automated monitoring capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless. Automated monitoring of remote access sessions allows organizations to detect cyber attacks and ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Audit:

Verify that the operating system monitors all remote access methods.

Check that remote access methods are being logged by running the following command:

```
# grep -E '(auth.*|authpriv.*|daemon.*)' /etc/rsyslog.conf  
auth.*;authpriv.*;daemon.* /var/log/secure
```

If "auth.", "authpriv." or "daemon.*" are not configured to be logged, this is a finding.

Remediation:

Configure the operating system to monitor all remote access methods by installing rsyslog with the following command:

```
# dnf install rsyslog
```

Then add or update the following lines to the "/etc/rsyslog.conf" file:

```
auth.*;authpriv.*;daemon.* /var/log/secure
```

The "rsyslog" service must be restarted for the changes to take effect. To restart the "rsyslog" service, run the following command:

```
# systemctl restart rsyslog.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230228

Rule ID: SV-230228r627750_rule

STIG ID: RHEL-08-010070

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.2.1.4 Ensure rsyslog Service is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Once the `rsyslog` package is installed it needs to be activated.

Rationale:

If the `rsyslog` service is not activated the system may default to the `syslogd` service or lack logging instead.

Audit:

Run the following command to verify `rsyslog` is enabled:

```
# systemctl is-enabled rsyslog  
enabled
```

Verify result is "enabled".

Remediation:

Run the following command to enable `rsyslog`:

```
# systemctl --now enable rsyslog
```

Additional Information:

Additional methods of enabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.2.1.5 Ensure rsyslog default file permissions configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

rsyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Audit:

Run the following command and verify that \$FileCreateMode is 0640 or more restrictive:

```
# grep ^\$FileCreateMode /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Remediation:

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and set \$FileCreateMode to 0640 or more restrictive:

```
$FileCreateMode 0640
```

References:

1. See the rsyslog.conf(5) man page for more information.

Additional Information:

You should also ensure this is not overridden with less restrictive settings in any /etc/rsyslog.d/* conf file.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.2.1.6 Ensure logging is configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via `rsyslog` (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Audit:

Review the contents of the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files to ensure appropriate logging is set. In addition, run the following command and verify that the log files are logging information:

```
# ls -l /var/log/
```

Remediation:

Edit the following lines in the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files as appropriate for your environment:

<code>*.emerg</code>	<code>:omusrmsg:*</code>
<code>auth,authpriv.*</code>	<code>/var/log/secure</code>
<code>mail.*</code>	<code>-/var/log/mail</code>
<code>mail.info</code>	<code>-/var/log/mail.info</code>
<code>mail.warning</code>	<code>-/var/log/mail.warn</code>
<code>mail.err</code>	<code>-/var/log/mail.err</code>
<code>news.crit</code>	<code>-/var/log/news/news.crit</code>
<code>news.err</code>	<code>-/var/log/news/news.err</code>
<code>news.notice</code>	<code>-/var/log/news/news.notice</code>
<code>*.=warning;*.=err</code>	<code>-/var/log/warn</code>
<code>*.crit</code>	<code>-/var/log/warn</code>
<code>*.*;mail.none;news.none</code>	<code>-/var/log/messages</code>
<code>local0,local1.*</code>	<code>-/var/log/localmessages</code>
<code>local2,local3.*</code>	<code>-/var/log/localmessages</code>
<code>local4,local5.*</code>	<code>-/var/log/localmessages</code>
<code>local6,local7.*</code>	<code>-/var/log/localmessages</code>

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

References:

1. See the rsyslog.conf(5) man page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.2.1.7 Ensure rsyslog is configured to send logs to a remote log host (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsyslog` utility supports the ability to send logs it gathers to a remote log host running `syslogd(8)` or to receive messages from remote hosts, reducing administrative overhead.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Audit:

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that logs are sent to a central host (where `loghost.example.com` is the name of your central log host):

```
# grep ".*.*[^I][^I]*@" /etc/rsyslog.conf /etc/rsyslog.d/*.conf  
*.* @@loghost.example.com
```

Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and add the following line (where `loghost.example.com` is the name of your central log host).

```
*.* @@loghost.example.com
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

References:

1. See the `rsyslog.conf(5)` man page for more information.

Additional Information:

The double "at" sign (`@@`) directs `rsyslog` to use TCP to send log messages to the server, which is a more reliable transport mechanism than the default UDP protocol.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.6 Deploy SIEM or Log Analytic tool Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.		●	●
v7	6.8 Regularly Tune SIEM On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.			●

4.2.1.8 Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

By default, `rsyslog` does not listen for log messages coming in from remote systems. The `ModLoad` tells `rsyslog` to load the `imtcp.so` module so it can listen over a network via TCP. The `InputTCPServerRun` option instructs `rsyslogd` to listen on the specified TCP port.

Rationale:

The guidance in the section ensures that remote log hosts are configured to only accept `rsyslog` data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote `rsyslog` messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

Audit:

Run the following commands and verify the resulting lines are uncommented on designated log hosts and commented or removed on all others:

```
# grep '$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
$ModLoad imtcp

# grep '$InputTCPServerRun' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
$InputTCPServerRun 514
```

Remediation:

For hosts that are designated as log hosts, edit the `/etc/rsyslog.conf` file and uncomment or add the following lines:

```
$ModLoad imtcp  
$InputTCPServerRun 514
```

For hosts that are not designated as log hosts, edit the `/etc/rsyslog.conf` file and comment or remove the following lines:

```
# $ModLoad imtcp  
# $InputTCPServerRun 514
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

References:

1. See the `rsyslog(8)` man page for more information.

Additional Information:

The `$ModLoad imtcp` line can have the `.so` extension added to the end of the module, or use the full path to the module.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.2.1.9 Ensure "rsyslog" is configured to log cron events (Automated)

Profile Applicability:

- STIG

Description:

Cron logging must be implemented.

Rationale:

Cron logging can be used to trace the successful or unsuccessful execution of cron jobs. It can also be used to spot intrusions into the use of the cron facility by unauthorized and malicious users.

Audit:

Verify that "rsyslog" is configured to log cron events with the following command:

Note: If another logging package is used, substitute the utility configuration file for "/etc/rsyslog.conf" or "/etc/rsyslog.d/*.conf" files.

```
# grep -s cron /etc/rsyslog.conf /etc/rsyslog.d/*.conf  
  
/etc/rsyslog.conf:*.info;mail.none;authpriv.none;cron.none /var/log/messages  
/etc/rsyslog.conf:# Log cron stuff  
/etc/rsyslog.conf:cron.* /var/log/cron
```

If the command does not return a response, check for cron logging all facilities with the following command.

```
# grep -s /var/log/messages /etc/rsyslog.conf /etc/rsyslog.d/*.conf  
  
/etc/rsyslog.conf:*.info;mail.none;authpriv.none;cron.none /var/log/messages
```

If "rsyslog" is not logging messages for the cron facility or all facilities, this is a finding.

Remediation:

Configure "rsyslog" to log all cron messages by adding or updating the following line to "/etc/rsyslog.conf" or a configuration file in the /etc/rsyslog.d/ directory:

```
cron.* /var/log/cron
```

The rsyslog daemon must be restarted for the changes to take effect:

```
# systemctl restart rsyslog.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230387

Rule ID: SV-230387r743996_rule

STIG ID: RHEL-08-030010

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.2.2 Configure journald

systemd-journald is a system service that collects and stores logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources: Kernel log messages, via kmsq

Any changes made to the systemd-journald configuration will require a re-start of systemd-journald

4.2.2.1 Ensure journald is configured to send logs to rsyslog (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Data from journald may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of journald logs, however, use of the rsyslog service provides a consistent means of log collection and export.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Audit:

Review `/etc/systemd/journald.conf` and verify that logs are forwarded to syslog

```
# grep -e ^\s*ForwardToSyslog /etc/systemd/journald.conf
ForwardToSyslog=yes
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
ForwardToSyslog=yes
```

References:

1. <https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf>

Additional Information:

This recommendation assumes that recommendation 4.2.1.5, "Ensure rsyslog is configured to send logs to a remote log host" has been implemented.

As noted in the journald man pages, journald logs may be exported to rsyslog either through the process mentioned here, or through a facility like `systemd-journald.service`. There are trade-offs involved in each implementation, where `ForwardToSyslog` will immediately capture all events (and forward to an external log server, if properly configured), but may not capture all boot-up activities. Mechanisms such as `systemd-journald.service`, on the other hand, will record bootup events, but may delay sending the information to rsyslog, leading to the potential for log manipulation prior to export. Be aware of the limitations of all tools employed to secure a system.

The main configuration file `/etc/systemd/journald.conf` is read before any of the custom `*.conf` files. If there are custom configs present, they override the main configuration parameters

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

4.2.2.2 Ensure journald is configured to compress large log files (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The journald system includes the capability of compressing overly large files to avoid filling up the system with logs or making the logs unmanageably large.

Rationale:

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

Audit:

Review `/etc/systemd/journald.conf` and verify that large files will be compressed:

```
# grep -e ^\s*Compress /etc/systemd/journald.conf
Compress=yes
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
Compress=yes
```

References:

1. <https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf>

Additional Information:

The main configuration file `/etc/systemd/journald.conf` is read before any of the custom `*.conf` files. If there are custom configs present, they override the main configuration parameters

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

4.2.2.3 Ensure journald is configured to write logfiles to persistent disk (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Data from journald may be stored in volatile memory or persisted locally on the server. Logs in memory will be lost upon a system reboot. By persisting logs to local disk on the server they are protected from loss.

Rationale:

Writing log data to disk will provide the ability to forensically reconstruct events which may have impacted the operations or security of a system even after a system crash or reboot.

Audit:

Review `/etc/systemd/journald.conf` and verify that logs are persisted to disk:

```
# grep -e ^\s*Storage /etc/systemd/journald.conf
Storage=persistent
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
Storage=persistent
```

References:

1. <https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf>

Additional Information:

The main configuration file `/etc/systemd/journald.conf` is read before any of the custom `*.conf` files. If there are custom configs present, they override the main configuration parameters

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.2.3 Ensure permissions on all logfiles are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Audit:

Run the following commands and verify that other has no permissions on any files and group does not have write or execute permissions on any files:

```
# find /var/log/ -type f -perm /g+wx,o+rwx -exec ls -l "{}" +
```

No output should be returned

Remediation:

Run the following commands to set permissions on all existing log files:

```
# find /var/log/ -type f -perm /g+wx,o+rwx -exec chmod g-wx,o-rwx "{}" +
```

Additional Information:

You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.3 Ensure logrotate is configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file `/etc/logrotate.d/syslog` is the configuration file used to rotate log files created by `syslog` or `rsyslog`.

Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

Audit:

Review `/etc/logrotate.conf` and `/etc/logrotate.d/*` and verify logs are rotated according to site policy.

Remediation:

Edit `/etc/logrotate.conf` and `/etc/logrotate.d/*` to ensure logs are rotated according to site policy.

Additional Information:

If no `maxage` setting is set for logrotate a situation can occur where logrotate is interrupted and fails to delete rotated logfiles. It is recommended to set this to a value greater than the longest any log file should exist on your system to ensure that any such logfile is removed but standard rotation settings are not overridden.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.	●	●	

4.4 Ensure administrators are notified if an audit processing failure occurs by modifying "/etc/aliases" (Automated)

Profile Applicability:

- STIG

Description:

The operating system's Information System Security Officer (ISSO) and System Administrator (SA) (at a minimum) must have mail aliases to be notified of an audit processing failure.

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

Verify that the administrators are notified in the event of an audit processing failure. Check that the "/etc/aliases" file has a defined value for "root".

```
# grep "postmaster:\s*root$" /etc/aliases
```

If the command does not return a line, or the line is commented out, ask the system administrator to indicate how they and the ISSO are notified of an audit process failure. If there is no evidence of the proper personnel being notified of an audit processing failure, this is a finding.

Remediation:

Configure the operating system to notify administrators in the event of an audit processing failure.

Add/update the following line in "/etc/aliases":

```
postmaster: root
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230389

Rule ID: SV-230389r627750_rule

STIG ID: RHEL-08-030030

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5 Access, Authentication and Authorization

5.1 Configure cron

5.1.1 Ensure cron daemon is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `cron` daemon is used to execute batch jobs on the system.

Rationale:

While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and `cron` is used to execute them.

Audit:

Run the the following command to verify `cron` is enabled:

```
# systemctl is-enabled crond  
enabled
```

Verify result is "enabled".

Remediation:

Run the following command to enable `cron`:

```
# systemctl --now enable crond
```

Additional Information:

Additional methods of enabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.1.2 Ensure permissions on /etc/crontab are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/crontab` file is used by `cron` to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file.

Rationale:

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group or other`:

```
# stat /etc/crontab
Access: (0600/-rw-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/crontab`:

```
# chown root:root /etc/crontab
# chmod og-rwx /etc/crontab
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This directory contains system cron jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group or other`:

```
# stat /etc/cron.hourly
Access: (0700/drwx-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.hourly`:

```
# chown root:root /etc/cron.hourly
# chmod og-rwx /etc/cron.hourly
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.1.4 Ensure permissions on /etc/cron.daily are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/cron.daily` directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat /etc/cron.daily
Access: (0700/drwx-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.daily`:

```
# chown root:root /etc/cron.daily
# chmod og-rwx /etc/cron.daily
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/cron.weekly` directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group or other`:

```
# stat /etc/cron.weekly
Access: (0700/drwx-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.weekly`:

```
# chown root:root /etc/cron.weekly
# chmod og-rwx /etc/cron.weekly
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/cron.monthly` directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group or other`:

```
# stat /etc/cron.monthly
Access: (0700/drwx-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.monthly`:

```
# chown root:root /etc/cron.monthly
# chmod og-rwx /etc/cron.monthly
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.1.7 Ensure permissions on /etc/cron.d are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/cron.d` directory contains system `cron` jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from `/etc/crontab`, but require more granular control as to when they run. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group or other`:

```
# stat /etc/cron.d
Access: (0700/drwx-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.d`:

```
# chown root:root /etc/cron.d
# chmod og-rwx /etc/cron.d
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.1.8 Ensure at/cron is restricted to authorized users (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure `/etc/cron.allow` and `/etc/at.allow` to allow specific users to use these services. If `/etc/cron.allow` or `/etc/at.allow` do not exist, then `/etc/at.deny` and `/etc/cron.deny` are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in `/etc/cron.allow` and `/etc/at.allow` are allowed to use at and cron. Note that even though a given user is not listed in `cron.allow`, cron jobs can still be run as that user. The `cron.allow` file only controls administrative access to the crontab command for scheduling and modifying cron jobs.

Rationale:

On many systems, only the system administrator is authorized to schedule `cron` jobs. Using the `cron.allow` file to control who can run `cron` jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Audit:

Run the following command to verify /etc/cron.deny doesn't exist:

```
# [ -e /etc/cron.deny ] && stat /etc/cron.deny  
Nothing should be returned
```

Run the following command to verify /etc/at.deny doesn't exist:

```
# [ -e /etc/at.deny ] && stat /etc/at.deny  
Nothing should be returned
```

Run the following command and verify **Uid** and **Gid** are both 0/root and **Access** does not grant permissions to group or other for /etc/cron.allow:

```
# stat /etc/cron.allow  
Access: (0600/-rw-----) Uid: (      0/    root)  Gid: (      0/    root)
```

Run the following command and verify **Uid** and **Gid** are both 0/root and **Access** does not grant permissions to group or other for /etc/at.allow:

```
# stat /etc/at.allow  
Access: (0600/-rw-----) Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to:

- **remove** /etc/cron.deny and /etc/at.deny
- **create, set permissions, and set and ownership for** /etc/cron.allow and /etc/at.allow:

```
# rm /etc/cron.deny  
# rm /etc/at.deny  
  
# touch /etc/cron.allow  
# touch /etc/at.allow  
  
# chmod og-rwx /etc/cron.allow  
# chmod og-rwx /etc/at.allow  
  
# chown root:root /etc/cron.allow  
# chown root:root /etc/at.allow
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	16 Account Monitoring and Control Account Monitoring and Control			

5.2 SSH Server Configuration

SSH is a secure, encrypted replacement for common login services such as `telnet`, `ftp`, `rlogin`, `rsh`, and `rcp`. It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

Note:

- The recommendations in this section only apply if the SSH daemon is installed on the system, if remote access is **not** required the SSH daemon can be removed and this section skipped.
- Once all configuration changes have been made to `/etc/ssh/sshd_config`, the `sshd` configuration must be reloaded:

Command to re-load the SSH daemon configuration:

```
# systemctl reload sshd
```

Command to remove the SSH daemon:

```
# dnf remove openssh-server
```

5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The /etc/ssh/sshd_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root.

Rationale:

The /etc/ssh/sshd_config file needs to be protected from unauthorized changes by non-privileged users.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to group or other:

```
# stat /etc/ssh/sshd_config
Access: (0600/-rw-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on /etc/ssh/sshd_config:

```
# chown root:root /etc/ssh/sshd_config
# chmod og-rwx /etc/ssh/sshd_config
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.2 Ensure SSH private key files have a passcode (Manual)

Profile Applicability:

- STIG

Description:

The operating system's certificate-based authentication must enforce authorized access to the corresponding private key.

Rationale:

If an unauthorized user obtains access to a private key without a passcode, that user would have unauthorized access to any system where the associated public key has been installed.

Audit:

Verify the SSH private key files have a passcode.

For each private key stored on the system, use the following command:

```
# ssh-keygen -y -f /path/to/file
```

If the contents of the key are displayed, this is a finding.

Remediation:

Create a new private and public key pair that utilizes a passcode with the following command:

```
# ssh-keygen -n [passphrase]
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230230

Rule ID: SV-230230r627750_rule

STIG ID: RHEL-08-010100

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.3 Ensure SSH access is limited (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

- AllowUsers:
 - The `AllowUsers` variable gives the system administrator the option of allowing specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of `user@host`.
- AllowGroups:
 - The `AllowGroups` variable gives the system administrator the option of allowing specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.
- DenyUsers:
 - The `DenyUsers` variable gives the system administrator the option of denying specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of `user@host`.
- DenyGroups:
 - The `DenyGroups` variable gives the system administrator the option of denying specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

Rationale:

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Audit:

Run the following commands and verify the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -Pi '^h*(allow|deny) (users|groups) \h+\H+(\h+.* )?$$'  
# grep -Pi '^h*(allow|deny) (users|groups) \h+\H+(\h+.* )?$$' /etc/ssh/sshd_config
```

Verify that the output of both commands matches at least one of the following lines:

```
allowusers <userlist>  
allowgroups <grouplist>  
denyusers <userlist>  
denygroups <grouplist>
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set one or more of the parameter as follows:

```
AllowUsers <userlist>
```

OR

```
AllowGroups <grouplist>
```

OR

```
DenyUsers <userlist>
```

OR

```
DenyGroups <grouplist>
```

Default Value:

None

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

5.2.4 Ensure permissions on SSH private host key files are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

An SSH private key is one of two files used in SSH public key authentication. In this authentication method, the possession of the private key is proof of identity. Only a private key that corresponds to a public key will be able to authenticate successfully. The private keys need to be stored and handled carefully, and no copies of the private key should be distributed.

Rationale:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated

Audit:

Note: Either mode 0640 with owner root and group ssh_keys OR mode 0600 with owner root and group root is acceptable

Run the following command and verify either:

Uid is 0/root and Gid is /ssh_keys and permissions 0640 or more restrictive:

Or

Uid is 0/root and Gid is 0/root and permissions are 0600 or more restrictive:

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec stat {} \;
```

Example output:

```
File: '/etc/ssh/ssh_host_rsa_key'
  Size: 1679          Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d  Inode: 8628138    Links: 1
Access: (0640/-rw-r----)  Uid: ( 0/      root)  Gid: ( 993/ssh_keys)
Access: 2018-10-22 18:24:56.861750616 +0000
Modify: 2018-10-22 18:24:56.861750616 +0000
Change: 2018-10-22 18:24:56.873750616 +0000
 Birth: -
  File: '/etc/ssh/ssh_host_ecdsa_key'
  Size: 227          Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d  Inode: 8631760    Links: 1
Access: (0640/-rw-r----)  Uid: ( 0/      root)  Gid: ( 993/ssh_keys)
Access: 2018-10-22 18:24:56.897750616 +0000
Modify: 2018-10-22 18:24:56.897750616 +0000
Change: 2018-10-22 18:24:56.905750616 +0000
 Birth: -
  File: '/etc/ssh/ssh_host_ed25519_key'
  Size: 387          Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d  Inode: 8631762    Links: 1
Access: (0640/-rw-r----)  Uid: ( 0/      root)  Gid: ( 993/ssh_keys)
Access: 2018-10-22 18:24:56.945750616 +0000
Modify: 2018-10-22 18:24:56.945750616 +0000
Change: 2018-10-22 18:24:56.957750616 +0000
 Birth: -
```

Remediation:

Run the following commands to set permissions, ownership, and group on the private SSH host key files:

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chmod u-x,g-wx,o-rwx {} \;
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chown root:ssh_keys {} \;
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide Version 1,
Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230287

Rule ID: SV-230287r743951_rule

STIG ID: RHEL-08-010490

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5.2.5 Ensure permissions on SSH public host key files are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

An SSH public key is one of two files used in SSH public key authentication. In this authentication method, a public key is a key that can be used for verifying digital signatures generated using a corresponding private key. Only a public key that corresponds to a private key will be able to authenticate successfully.

Rationale:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Audit:

Run the following command and verify Access does not grant write or execute permissions to group or other for all returned files:

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec stat {} \;
```

Example output:

```
File: '/etc/ssh/ssh_host_rsa_key.pub'
  Size: 382          Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d  Inode: 8631758    Links: 1
Access: (0644/-rw-r--r--)
  Uid: ( 0/      root)  Gid: ( 0/      root)
Access: 2018-10-22 18:24:56.861750616 +0000
Modify: 2018-10-22 18:24:56.861750616 +0000
Change: 2018-10-22 18:24:56.881750616 +0000
 Birth: -
File: '/etc/ssh/ssh_host_ecdsa_key.pub'
  Size: 162          Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d  Inode: 8631761    Links: 1
Access: (0644/-rw-r--r--)
  Uid: ( 0/      root)  Gid: ( 0/      root)
Access: 2018-10-22 18:24:56.897750616 +0000
Modify: 2018-10-22 18:24:56.897750616 +0000
Change: 2018-10-22 18:24:56.917750616 +0000
 Birth: -
File: '/etc/ssh/ssh_host_ed25519_key.pub'
  Size: 82           Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d  Inode: 8631763    Links: 1
Access: (0644/-rw-r--r--)
  Uid: ( 0/      root)  Gid: ( 0/      root)
Access: 2018-10-22 18:24:56.945750616 +0000
Modify: 2018-10-22 18:24:56.945750616 +0000
Change: 2018-10-22 18:24:56.961750616 +0000
 Birth: -
```

Remediation:

Run the following commands to set permissions and ownership on the SSH host public key files

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chmod u-x,go-wx {} \;
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chown root:root {} \;
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230286

Rule ID: SV-230286r627750_rule

STIG ID: RHEL-08-010480

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.6 Ensure SSH LogLevel is appropriate (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`INFO` level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

`VERBOSE` level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments.

Rationale:

SSH provides several logging levels with varying amounts of verbosity. `DEBUG` is specifically **not** recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

Audit:

Run the following command and verify that output matches `loglevel VERBOSE` or `loglevel INFO`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep loglevel  
loglevel VERBOSE or loglevel INFO
```

Run the following command and verify the output matches:

```
# grep -i 'loglevel' /etc/ssh/sshd_config | grep -Evi '(VERBOSE|INFO)'
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LogLevel VERBOSE
```

Or

```
LogLevel INFO
```

Default Value:

LogLevel INFO

References:

1. https://www.ssh.com/ssh/sshd_config/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

5.2.7 Ensure SSH X11 forwarding is disabled (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 2 - Server
- STIG

Description:

The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.

Rationale:

Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i x11forwarding  
x11forwarding no
```

Run the following command and verify that the output matches:

```
# grep -Ei '^s*x11forwarding\s+yes' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
x11Forwarding no
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230555

Rule ID: SV-230555r627750_rule

STIG ID: RHEL-08-040340

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

5.2.8 Ensure SSH MaxAuthTries is set to 4 or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxAuthTries` parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the `syslog` file detailing the login failure.

Rationale:

Setting the `MaxAuthTries` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Audit:

Run the following command and verify that output `MaxAuthTries` is 4 or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep maxauthtries  
maxauthtries 4
```

Run the following command and verify that the output:

```
# grep -Ei '^\\s*maxauthtries\\s+([5-9]|1-9)[0-9]+)' /etc/ssh/sshd_config  
Nothing is returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxAuthTries 4
```

Default Value:

`MaxAuthTries 6`

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			

5.2.9 Ensure SSH IgnoreRhosts is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `IgnoreRhosts` parameter specifies that `.rhosts` and `.shosts` files will not be used in `RhostsRSAAuthentication` or `HostbasedAuthentication`.

Rationale:

Setting this parameter forces users to enter a password when authenticating with ssh.

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep ignorerhosts  
ignorerhosts yes
```

Run the following command and verify the output:

```
# grep -Ei '^s*ignorerhosts\s+no\b' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
IgnoreRhosts yes
```

Default Value:

`IgnoreRhosts yes`

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

5.2.10 Ensure SSH HostbasedAuthentication is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `HostbasedAuthentication` parameter specifies if authentication is allowed through trusted hosts via the user of `.rhosts`, or `/etc/hosts.equiv`, along with successful public key client host authentication. This option only applies to SSH Protocol Version 2.

Rationale:

Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, disabling the ability to use `.rhosts` files in SSH provides an additional layer of protection.

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep hostbasedauthentication  
hostbasedauthentication no
```

Run the following command and verify the output matches:

```
# grep -Ei '^s*HostbasedAuthentication\s+yes' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
HostbasedAuthentication no
```

Default Value:

HostbasedAuthentication no

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

5.2.11 Ensure SSH root login is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `PermitRootLogin` parameter specifies if the root user can log in using ssh. The default is no.

Rationale:

Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via `sudo` or `su`. This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permitrootlogin  
permitrootlogin no
```

Run the following command and verify the output:

```
# grep -Ei '^s*PermitRootLogin\s+yes' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitRootLogin no
```

Default Value:

`PermitRootLogin without-password`

References:

1. `SSHD_CONFIG(5)`

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230296

Rule ID: SV-230296r627750_rule

STIG ID: RHEL-08-010550

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

5.2.12 Ensure SSH PermitEmptyPasswords is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PermitEmptyPasswords` parameter specifies if the SSH server allows login to accounts with empty password strings.

Rationale:

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permitemptypasswords  
permitemptypasswords no
```

Run the following command and verify the output:

```
# grep -Ei '^s*PermitEmptyPasswords\s+yes' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitEmptyPasswords no
```

Default Value:

PermitEmptyPasswords no

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

5.2.13 Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity (Automated)

Profile Applicability:

- STIG

Description:

The SSH daemon must be configured with a timeout interval.

Rationale:

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

RHEL 8 operating systems utilize "/etc/ssh/sshd_config" for configurations of OpenSSH. Within the sshd_config the product of the values of "ClientAliveInterval" and "ClientAliveCountMax" are used to establish the inactivity threshold. The "ClientAliveInterval" is a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The "ClientAliveCountMax" is the number of client alive messages that may be sent without sshd receiving any messages back from the client. If this threshold is met, sshd will disconnect the client. For more information on these settings and others, refer to the "sshd_config" man pages.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000126-GPOS-00066, SRG-OS-000279-GPOS-00109

Audit:

Verify all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity.

Check that the "ClientAliveInterval" variable is set to a value of "600" or less by performing the following command:

```
# grep -i clientalive /etc/ssh/sshd_config  
  
ClientAliveInterval 600  
ClientAliveCountMax 0
```

If "ClientAliveInterval" does not exist, does not have a value of "600" or less in "/etc/ssh/sshd_config", or is commented out, this is a finding.

Remediation:

Configure the operating system to automatically terminate all network connections associated with SSH traffic at the end of a session or after 10 minutes of inactivity.

Modify or append the following lines in the "/etc/ssh/sshd_config" file:

```
ClientAliveInterval 600
```

In order for the changes to take effect, the SSH daemon must be restarted.

```
# systemctl restart sshd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244525

Rule ID: SV-244525r743824_rule

STIG ID: RHEL-08-010201

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

5.2.14 Ensure SSH PermitUserEnvironment is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The `PermitUserEnvironment` option allows users to present environment options to the `ssh` daemon.

Rationale:

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has `ssh` executing trojan'd programs)

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permituserenvironment  
permituserenvironment no
```

Run the following command and verify the output:

```
# grep -Ei '^\\s*PermitUserEnvironment\\s+yes' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitUserEnvironment no
```

Default Value:

PermitUserEnvironment no

References:

1. `SSHD_CONFIG(5)`

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230330

Rule ID: SV-230330r646870_rule

STIG ID: RHEL-08-010830

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.15 Ensure SSH Idle Timeout Interval is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of ssh sessions.

- `ClientAliveInterval` sets a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client.
- `ClientAliveCountMax` sets the number of client alive messages which may be sent without sshd receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. The default value is 3.
 - The client alive messages are sent through the encrypted channel
 - Setting `ClientAliveCountMax` to 0 disables connection termination

Example: The default value is 3. If `ClientAliveInterval` is set to 15, and `ClientAliveCountMax` is left at the default, unresponsive SSH clients will be disconnected after approximately 45 seconds

Rationale:

Having no timeout value associated with a connection could allow an unauthorized user access to another user's ssh session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value reduces this risk.

- The recommended `ClientAliveInterval` setting is no greater than 900 seconds (15 minutes)
- The recommended `ClientAliveCountMax` setting is 0
- At the 15 minute interval, if the ssh session is inactive, the session will be terminated.

Impact:

In some cases this setting may cause termination of long-running scripts over SSH or remote automation tools which rely on SSH. In developing the local site policy, the requirements of such scripts should be considered and appropriate `ServerAliveInterval` and `ClientAliveInterval` settings should be calculated to insure operational continuity.

Audit:

Run the following commands and verify ClientAliveInterval is between 1 and 900:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep clientaliveinterval  
clientaliveinterval 900
```

Run the following command and verify ClientAliveCountMax is 0:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep clientalivecountmax  
clientalivecountmax 3
```

Run the following commands and verify the output:

```
# grep -Ei '^s*ClientAliveInterval\s+(0|9[0-9][1-9]|1[0-9][0-9][0-9][0-9]+|1[6-9]m|[2-9][0-9]m|[1-9][0-9][0-9]m)\b' /etc/ssh/sshd_config  
Nothing should be returned  
  
# grep -Ei '^s*ClientAliveCountMax\s+([1-9]|1[0-9]+)\b' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the /etc/ssh/sshd_config file to set the parameters according to site policy. This should include ClientAliveInterval between 1 and 900 and ClientAliveCountMax of 0:

```
ClientAliveInterval 900  
ClientAliveCountMax 0
```

Default Value:

ClientAliveInterval 0
ClientAliveCountMax 3

References:

1. https://man.openbsd.org/sshd_config

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230244

Rule ID: SV-230244r743934_rule

STIG ID: RHEL-08-010200

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

5.2.16 Ensure SSH LoginGraceTime is set to one minute or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `LoginGraceTime` parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access.

Rationale:

Setting the `LoginGraceTime` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections. While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

Audit:

Run the following command and verify that output `LoginGraceTime` is between 1 and 60 seconds or 1m:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep logingracetime  
logingracetime 60
```

Run the following command and verify the output:

```
# grep -Ei '^s*LoginGraceTime\s+(0|6[1-9]|7-9 [0-9] | [1-9] [0-9] [0-9]+|^1m)' /etc/ssh/sshd_config
```

Nothing should be returned

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LoginGraceTime 60
```

Default Value:

`LoginGraceTime 120`

References:

1. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.17 Ensure SSH warning banner is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `Banner` parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

Rationale:

Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep banner  
banner /etc/issue.net
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Banner /etc/issue.net
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.18 Ensure SSH PAM is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

UsePAM Enables the Pluggable Authentication Module interface. If set to “yes” this will enable PAM authentication using ChallengeResponseAuthentication and PasswordAuthentication in addition to PAM account and session module processing for all authentication types

Rationale:

When usePAM is set to yes, PAM runs through account and session types properly. This is important if you want to restrict access to services based off of IP, time or other factors of the account. Additionally, you can make sure users inherit certain environment variables on login or disallow access to the server

Impact:

If UsePAM is enabled, you will not be able to run sshd(8) as a non-root user.

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i usepam  
usepam yes
```

Run the following command and verify the output:

```
# grep -Ei '^s*UsePAM\s+no' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

```
UsePAM yes
```

Default Value:

usePAM yes

References:

1. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.19 Ensure SSH AllowTcpForwarding is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

SSH port forwarding is a mechanism in SSH for tunneling application ports from the client to the server, or servers to clients. It can be used for adding encryption to legacy applications, going through firewalls, and some system administrators and IT professionals use it for opening backdoors into the internal network from their home machines

Rationale:

Leaving port forwarding enabled can expose the organization to security risks and backdoors.

SSH connections are protected with strong encryption. This makes their contents invisible to most deployed network monitoring and traffic filtering solutions. This invisibility carries considerable risk potential if it is used for malicious purposes such as data exfiltration.

Cybercriminals or malware could exploit SSH to hide their unauthorized communications, or to exfiltrate stolen data from the target network

Impact:

SSH tunnels are widely used in many corporate environments that employ mainframe systems as their application backends. In those environments the applications themselves may have very limited native support for security. By utilizing tunneling, compliance with SOX, HIPAA, PCI-DSS, and other standards can be achieved without having to modify the applications.

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i allowtcpforwarding  
allowtcpforwarding no
```

Run the following command and verify the output:

```
# grep -Ei '^s*AllowTcpForwarding\s+yes' /etc/ssh/sshd_config
```

Nothing should be returned

Remediation:

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

AllowTcpForwarding no

Default Value:

AllowTcpForwarding yes

References:

1. <https://www.ssh.com/ssh/tunneling/example>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	●	●	●

5.2.20 Ensure SSH MaxStartups is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxStartups` parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.

Rationale:

To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of `MaxStartups` to protect availability of `sshd` logins and prevent overwhelming the daemon.

Audit:

Run the following command and verify that output `MaxStartups` is `10:30:60` or more restrictive:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i maxstartups  
maxstartups 10:30:60
```

Run the following command and verify the output:

```
# grep -Ei '^s*maxstartups\s+(((1[1-9]|1[1-9][0-9][0-9]+):([0-9]+):([0-9]+))|(([0-9]+):(3[1-9]|[4-9][0-9]|1[1-9][0-9][0-9]+):([0-9]+))|(([0-9]+):([0-9]+):(6[1-9]|[7-9][0-9]|1[1-9][0-9][0-9]+)))' /etc/ssh/sshd_config
```

Nothing should be returned

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
maxstartups 10:30:60
```

Default Value:

MaxStartups 10:30:100

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.21 Ensure SSH MaxSessions is set to 4 or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxSessions` parameter specifies the maximum number of open sessions permitted from a given connection.

Rationale:

To protect a system from denial of service due to a large number of concurrent sessions, use the rate limiting function of `MaxSessions` to protect availability of `sshd` logins and prevent overwhelming the daemon.

Audit:

Run the following command and verify that output `MaxSessions` is 10 or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i maxsessions  
maxsessions 10
```

Run the following command and verify the output:

```
grep -Ei '^s*MaxSessions\s+(1[1-9]|2[0-9]|1[0-9][0-9]|1[0-9][0-9][0-9]+)' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxSessions 10
```

Default Value:

`MaxSessions 10`

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.22 Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms (Automated)

Profile Applicability:

- STIG

Description:

The SSH server must be configured to use only Message Authentication Codes (MACs) employing FIPS 140-2 validated cryptographic hash algorithms.

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 8 operating systems incorporate system-wide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the /etc/sysconfig/sshd file. The employed algorithms can be viewed in the /etc/crypto-policies/back-ends/opensshserver.config file.

The system will attempt to use the first hash presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest hash available to secure the SSH connection.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000125-GPOS-00065

Audit:

Verify the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms with the following command:

```
# grep -i macs /etc/crypto-policies/back-ends/opensslserver.config  
-oMACS=hmac-sha2-512,hmac-sha2-256
```

If the MACs entries in the "opensslserver.config" file have any hashes other than "hmac-sha2-512" and "hmac-sha2-256", the order differs from the example above, they are missing, or commented out, this is a finding.

Remediation:

Configure the SSH server to use only MACs employing FIPS 140-2-approved algorithms by updating the "/etc/crypto-policies/back-ends/opensslserver.config" file with the following line:

```
-oMACS=hmac-sha2-512,hmac-sha2-256
```

A reboot is required for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230251

Rule ID: SV-230251r743937_rule

STIG ID: RHEL-08-010290

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v7	<p>14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.</p>		●	●
v7	<p>16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.</p>		●	●

5.2.23 Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement DoD-approved encryption to protect the confidentiality of SSH server connections.

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 8 operating systems incorporate system-wide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the /etc/sysconfig/sshd file. The employed algorithms can be viewed in the /etc/crypto-policies/back-ends/opensshserver.config file.

The system will attempt to use the first hash presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest hash available to secure the SSH connection.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000125-GPOS-00065

Audit:

Verify the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms with the following command:

```
# grep -i ciphers /etc/crypto-policies/back-ends/opensshserver.config  
CRYPTO_POLICY=' -oCiphers=aes256-ctr,aes192-ctr,aes128-ctr'
```

If the cipher entries in the "opensshserver.config" file have any ciphers other than "aes256-ctr,aes192-ctr,aes128-ctr", the order differs from the example above, they are missing, or commented out, this is a finding.

Remediation:

Configure the RHEL 8 SSH server to use only ciphers employing FIPS 140-2-approved algorithms by updating the "/etc/crypto-policies/back-ends/opensshserver.config" file with the following line:

```
-oCiphers=aes256-ctr,aes192-ctr,aes128-ctr
```

A reboot is required for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230252

Rule ID: SV-230252r743940_rule

STIG ID: RHEL-08-010291

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

5.2.24 Ensure the SSH server uses strong entropy (Automated)

Profile Applicability:

- STIG

Description:

Administrators must ensure the SSH server uses strong entropy.

Rationale:

The most important characteristic of a random number generator is its randomness, namely its ability to deliver random numbers that are impossible to predict. Entropy in computer security is associated with the unpredictability of a source of randomness. The random source with high entropy tends to achieve a uniform distribution of random values.

Random number generators are one of the most important building blocks of cryptosystems.

The SSH implementation in RHEL 8 operating systems uses the OPENSSL library, which does not use high-entropy sources by default. By using the "SSH_USE_STRONG_RNG" environment variable the OPENSSL random generator is reseeded from "/dev/random".

This setting is not recommended on computers without the hardware random generator because insufficient entropy causes the connection to be blocked until enough entropy is available.

Audit:

Verify the operating system SSH server uses strong entropy with the following command:
Note: If the operating system is RHEL versions 8.0 or 8.1, this requirement is not applicable.

```
# grep -i ssh_use_strong_rng /etc/sysconfig/sshd  
SSH_USE_STRONG_RNG=32
```

If the "SSH_USE_STRONG_RNG" line does not equal "32", is commented out or missing, this is a finding.

Remediation:

Configure the operating system SSH server to use strong entropy.
Add or modify the following line in the "/etc/sysconfig/sshd" file.

```
SSH_USE_STRONG_RNG=32
```

The SSH service must be restarted for changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230253

Rule ID: SV-230253r627750_rule

STIG ID: RHEL-08-010292

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.25 Ensure system-wide crypto policy is not over-ridden (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

System-wide Crypto policy can be over-ridden or opted out of for openSSH

Rationale:

Over-riding or opting out of the system-wide crypto policy could allow for the use of less secure Ciphers, MACs, KexAlgoritms and GSSAPIKexAlgorithm

Audit:

Run the following command:

```
# grep -i '^s*CRYPTO_POLICY=' /etc/sysconfig/sshd
```

No output should be returned.

Remediation:

Run the following commands:

```
# sed -ri "s/^s*(CRYPTO_POLICY\s*=.*$)/#\ \1/" /etc/sysconfig/sshd
# systemctl reload sshd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

5.2.26 Ensure the SSH daemon performs strict mode checking of home directory configuration files (Automated)

Profile Applicability:

- STIG

Description:

The operating system's SSH daemon must perform strict mode checking of home directory configuration files.

Rationale:

If other users have access to modify user-specific SSH configuration files, they may be able to log on to the system as another user.

Audit:

Ensure the SSH daemon performs strict mode checking of home directory configuration files with the following command:

```
# grep -i strictmodes /etc/ssh/sshd_config  
StrictModes yes
```

If "StrictModes" is set to "no", is missing, or the returned line is commented out, this is a finding.

Remediation:

Configure SSH to perform strict mode checking of home directory configuration files. Uncomment the "StrictModes" keyword in "/etc/ssh/sshd_config" and set the value to "yes":

```
StrictModes yes
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
# systemctl restart sshd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230288

Rule ID: SV-230288r627750_rule

STIG ID: RHEL-08-010500

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.27 Ensure the SSH daemon performs compression after a user successfully authenticates (Automated)

Profile Applicability:

- STIG

Description:

The operating system's SSH daemon must not allow compression or must only allow compression after successful authentication.

Rationale:

If compression is allowed in an SSH connection prior to authentication, vulnerabilities in the compression software could result in compromise of the system from an unauthenticated connection, potentially with root privileges.

Audit:

Verify the SSH daemon performs compression after a user successfully authenticates with the following command:

```
# grep -i compression /etc/ssh/sshd_config  
Compression delayed
```

If the "Compression" keyword is set to "yes", is missing, or the returned line is commented out, this is a finding.

Remediation:

Uncomment the "Compression" keyword in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) on the system and set the value to "delayed" or "no":

```
Compression no
```

The SSH service must be restarted for changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230289

Rule ID: SV-230289r743954_rule

STIG ID: RHEL-08-010510

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.28 Ensure the SSH daemon does not allow authentication using known host's authentication (Automated)

Profile Applicability:

- STIG

Description:

The operating system's SSH daemon must not allow authentication using known host's authentication.

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

Verify the SSH daemon does not allow authentication using known host's authentication with the following command:

```
# grep -i IgnoreUserKnownHosts /etc/ssh/sshd_config  
IgnoreUserKnownHosts yes
```

If the value is returned as "no", the returned line is commented out, or no output is returned, this is a finding.

Remediation:

Configure the SSH daemon to not allow authentication using known host's authentication.

Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "yes":

```
IgnoreUserKnownHosts yes
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
# systemctl restart sshd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230290

Rule ID: SV-230290r627750_rule

STIG ID: RHEL-08-010520

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.29 Ensure the SSH daemon does not allow Kerberos authentication (Automated)

Profile Applicability:

- STIG

Description:

The operating system's SSH daemon must not allow Kerberos authentication, except to fulfill documented and validated mission requirements.

Rationale:

Configuring these settings for the SSH daemon provides additional assurance that remote logon via SSH will not use unused methods of authentication, even in the event of misconfiguration elsewhere.

Audit:

Verify the SSH daemon does not allow Kerberos authentication with the following command:

```
# grep -i KerberosAuthentication /etc/ssh/sshd_config  
KerberosAuthentication no
```

If the value is returned as "yes", the returned line is commented out, no output is returned, or has not been documented with the ISSO, this is a finding.

Remediation:

Configure the SSH daemon to not allow Kerberos authentication.

Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "no":

```
KerberosAuthentication no
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
# systemctl restart sshd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230291

Rule ID: SV-230291r743957_rule

STIG ID: RHEL-08-010521

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.30 Ensure null passwords cannot be used (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not allow accounts configured with blank or null passwords.

Rationale:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Audit:

To verify that null passwords cannot be used, run the following command:

```
# grep -i permitemptypasswords /etc/ssh/sshd_config  
PermitEmptyPasswords no
```

If "PermitEmptyPasswords" is set to "yes", this is a finding.

Remediation:

Edit the following line in "etc/ssh/sshd_config" to prevent logons with empty passwords:

```
PermitEmptyPasswords no
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
# systemctl restart sshd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230380

Rule ID: SV-230380r743993_rule

STIG ID: RHEL-08-020330

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

5.2.31 Ensure SSH provides users with feedback on when account accesses last occurred (Automated)

Profile Applicability:

- STIG

Description:

The operating system must display the date and time of the last successful account logon upon an SSH logon.

Rationale:

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

Audit:

Verify SSH provides users with feedback on when account accesses last occurred with the following command:

```
# grep -i printlastlog /etc/ssh/sshd_config  
PrintLastLog yes
```

If the "PrintLastLog" keyword is set to "no", is missing, or is commented out, this is a finding.

Remediation:

Configure SSH to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/sshd" or in the "sshd_config" file used by the system (" /etc/ssh/sshd_config" will be used in the example) (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor).

Modify the "PrintLastLog" line in "/etc/ssh/sshd_config" to match the following:

```
PrintLastLog yes
```

The SSH service must be restarted for changes to "sshd_config" to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230382

Rule ID: SV-230382r627750_rule

STIG ID: RHEL-08-020350

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.32 Ensure SSH is loaded and active (Automated)

Profile Applicability:

- STIG

Description:

All networked systems must have and implement SSH to protect the confidentiality and integrity of transmitted and received information, as well as information during preparation for transmission.

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Verify SSH is loaded and active with the following command:

```
# systemctl status sshd

sshd.service - OpenSSH server daemon
Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled)
Active: active (running) since Tue 2015-11-17 15:17:22 EST; 4 weeks 0 days
ago
Main PID: 1348 (sshd)
CGroup: /system.slice/sshd.service
1053 /usr/sbin/sshd -D
```

If "sshd" does not show a status of "active" and "running", this is a finding.

Remediation:

Configure the SSH service to automatically start after reboot with the following command:

```
# systemctl enable sshd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230526

Rule ID: SV-230526r744032_rule

STIG ID: RHEL-08-040160

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.			
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

5.2.33 Ensure the SSH server is configured to force frequent session key renegotiation (Automated)

Profile Applicability:

- STIG

Description:

The operating system must force a frequent session key renegotiation for SSH connections to the server.

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Session key regeneration limits the chances of a session key becoming compromised.
Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000420-GPOS-00186, SRG-OS-000424-GPOS-00188

Audit:

Verify the SSH server is configured to force frequent session key renegotiation with the following command:

```
# grep -i RekeyLimit /etc/ssh/sshd_config
RekeyLimit 1G 1h
```

If "RekeyLimit" does not have a maximum data amount and maximum time defined, is missing or commented out, this is a finding.

Remediation:

Configure the system to force a frequent session key renegotiation for SSH connections to the server by add or modifying the following line in the "/etc/ssh/sshd_config" file:

```
RekeyLimit 1G 1h
```

Restart the SSH daemon for the settings to take effect.

```
# systemctl restart sshd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230527

Rule ID: SV-230527r627750_rule

STIG ID: RHEL-08-040161

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.34 Ensure the SSH daemon prevents remote hosts from connecting to the proxy display (Automated)

Profile Applicability:

- STIG

Description:

The SSH daemon must prevent remote hosts from connecting to the proxy display.

Rationale:

When X11 forwarding is enabled, there may be additional exposure to the server and client displays if the sshd proxy display is configured to listen on the wildcard address. By default, sshd binds the forwarding server to the loopback address and sets the hostname part of the DIPSLAY environment variable to localhost. This prevents remote hosts from connecting to the proxy display.

Audit:

Verify the SSH daemon prevents remote hosts from connecting to the proxy display.

Check the SSH X11UseLocalhost setting with the following command:

```
# grep -i x11uselocalhost /etc/ssh/sshd_config
X11UseLocalhost yes
```

If the "X11UseLocalhost" keyword is set to "no", is missing, or is commented out, this is a finding.

Remediation:

Configure the SSH daemon to prevent remote hosts from connecting to the proxy display.

Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for the "X11UseLocalhost" keyword and set its value to "yes" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

```
X11UseLocalhost yes
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230556

Rule ID: SV-230556r627750_rule

STIG ID: RHEL-08-040341

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.35 Ensure system-wide crypto policies are in effect (Automated)

Profile Applicability:

- STIG

Description:

The SSH daemon must be configured to use system-wide crypto policies.

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 8 operating systems incorporate system-wide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the "/etc/sysconfig/sshd" file. The employed algorithms can be viewed in the "/etc/crypto-policies/back-ends" directory.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000125-GPOS-00065

Audit:

Verify that system-wide crypto policies are in effect:

```
# grep -i crypto_policy /etc/sysconfig/sshd
# crypto_policy=
```

If the "crypto_policy" is uncommented, this is a finding.

Remediation:

Configure the SSH daemon to use system-wide crypto policies by adding the following line to /etc/sysconfig/sshd:

```
# crypto_policy=
```

A reboot is required for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244526

Rule ID: SV-244526r743827_rule

STIG ID: RHEL-08-010287

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.			

5.2.36 Ensure the SSH daemon does not allow GSSAPI authentication (Automated)

Profile Applicability:

- STIG

Description:

The SSH daemon must not allow GSSAPI authentication, except to fulfill documented and validated mission requirements.

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

Verify the SSH daemon does not allow GSSAPI authentication with the following command:

```
# grep -i GSSAPIAuthentication /etc/ssh/sshd_config  
GSSAPIAuthentication no
```

If the value is returned as "yes", the returned line is commented out, no output is returned, or has not been documented with the ISSO, this is a finding.

Remediation:

Configure the SSH daemon to not allow GSSAPI authentication.

Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "no":

```
GSSAPIAuthentication no
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
# systemctl restart sshd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244528

Rule ID: SV-244528r743833_rule

STIG ID: RHEL-08-010522

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.2.37 Ensure SSH is installed (Automated)

Profile Applicability:

- STIG

Description:

All networked systems must have SSH installed.

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Verify SSH is installed with the following command:

```
# dnf list installed openssh-server  
openssh-server.x86_64 8.0p1-5.el8 @anaconda
```

If the "SSH server" package is not installed, this is a finding.

Remediation:

Install SSH packages onto the host with the following command:

```
# dnf install openssh-server.x86_64
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244549

Rule ID: SV-244549r743896_rule

STIG ID: RHEL-08-040159

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

5.2.38 Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity (Automated)

Profile Applicability:

- STIG

Description:

The SSH daemon must be configured with a timeout interval.

Rationale:

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

RHEL 8 operating systems utilize "/etc/ssh/sshd_config" for configurations of OpenSSH. Within the sshd_config the product of the values of "ClientAliveInterval" and "ClientAliveCountMax" are used to establish the inactivity threshold. The "ClientAliveInterval" is a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The "ClientAliveCountMax" is the number of client alive messages that may be sent without sshd receiving any messages back from the client. If this threshold is met, sshd will disconnect the client. For more information on these settings and others, refer to the "sshd_config" man pages.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000126-GPOS-00066, SRG-OS-000279-GPOS-00109

Audit:

Verify all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity.

Check that the "ClientAliveInterval" variable is set to a value of "600" or less by performing the following command:

```
# grep -i clientalive /etc/ssh/sshd_config  
  
ClientAliveInterval 600  
ClientAliveCountMax 0
```

If "ClientAliveInterval" does not exist, does not have a value of "600" or less in "/etc/ssh/sshd_config", or is commented out, this is a finding.

Remediation:

Configure the operating system to automatically terminate all network connections associated with SSH traffic at the end of a session or after 10 minutes of inactivity.

Modify or append the following lines in the "/etc/ssh/sshd_config" file:

```
ClientAliveInterval 600
```

In order for the changes to take effect, the SSH daemon must be restarted.

```
# systemctl restart sshd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244525

Rule ID: SV-244525r743824_rule

STIG ID: RHEL-08-010201

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

5.3 Configure authselect

Authselect is a utility that simplifies the configuration of user authentication on a CentOS Linux host. Authselect offers two ready-made profiles that can be universally used with all modern identity management systems

Authselect makes testing and troubleshooting easy because it only modifies files in these directories:

- /etc/nsswitch.conf
- /etc/pam.d/* files
- /etc/dconf/db/distro.d/* files

Notes:

- **Do not use authselect if your host is part of CentOS Linux Identity Management or Active Directory.** The ipa-client-install command, called when joining your host to a CentOS Identity Management domain, takes full care of configuring authentication on your host. Similarly the realm join command, called when joining your host to an Active Directory domain, takes full care of configuring authentication on your host.
- You can create and deploy a custom profile by customizing one of the default profiles, the sssd, winbind, or the nis profile. This is particularly useful if modifying a ready-made authselect profile is not enough for your needs. When you deploy a custom profile, the profile is applied to every user logging into the given host. This would be the recommended method, so that the existing profiles can remain unmodified.

Example of creating a custom authselect profile called custom-profile

```
# authselect create-profile custom-profile -b sssd --symlink-meta
```

5.3.1 Create custom authselect profile (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A custom profile can be created by copying and customizing one of the default profiles. The default profiles include: sssd, winbind, or the nis.

Rationale:

A custom profile is required to customize many of the pam options

Audit:

Run the following command:

```
# authselect current | grep "Profile ID: custom"  
Profile ID: custom/<custom profile name>
```

Verify that the custom profile follows local site policy

Remediation:

Run the following command to create a custom authselect profile:

```
# authselect create-profile <custom-profile name> -b <default profile to  
copy>
```

Example:

```
# authselect create-profile custom-profile -b sssd --symlink-meta
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.3.2 Select authselect profile (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

You can select a profile for the authselect utility for a specific host. The profile will be applied to every user logging into the host.

You can create and deploy a custom profile by customizing one of the default profiles, the sssd, winbind, or the nis profile.

Rationale:

When you deploy a profile, the profile is applied to every user logging into the given host

Audit:

Run the following command and verify that the current custom authselect profile follows local site policy:

```
# authselect current
```

Output should be similar to:

```
Profile ID: <custom-profile name>
Enabled features:
- with-sudo
- with-faillock
- without-nullok
```

Remediation:

Run the following command to select a custom authselect profile

```
# authselect select custom/<CUSTOM PROFILE NAME> {with-<OPTIONS>}
```

Example:

```
# authselect select custom/custom-profile with-sudo with-faillock without-
nullok
```

References:

1. Using authselect on a Red Hat Enterprise Linux host

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

5.3.3 Ensure authselect includes with-faillock (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The pam_faillock.so module maintains a list of failed authentication attempts per user during a specified interval and locks the account in case there were more than deny consecutive failed authentications. It stores the failure records into per-user files in the tally directory

Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Audit:

Run the following commands to verify that faillock is enabled

```
# grep pam_faillock.so /etc/authselect/password-auth /etc/authselect/system-auth
```

Output should be similar to:

```
/etc/authselect/password-auth:auth      required
pam_faillock.so preauth silent
/etc/authselect/password-auth:auth      required
pam_faillock.so authfail
/etc/authselect/password-auth:account   required
pam_faillock.so
/etc/authselect/system-auth:auth        required
pam_faillock.so preauth silent
/etc/authselect/system-auth:auth        required
pam_faillock.so authfail
/etc/authselect/system-auth:account    required
pam_faillock.so
```

Remediation:

Run the following command to include the `with-faillock` option

```
# authselect select <PROFILE NAME> with-faillock
```

Example:

```
# authselect select custom/custom-profile with-sudo with-faillock without-nullok
```

References:

1. faillock(8) - Linux man page

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	●	●	●

5.4 Configure PAM

PAM (Pluggable Authentication Modules) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the `/etc/pam.d` directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

5.4.1 Ensure password creation requirements are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more. The following are definitions of the pam_pwquality.so options.

- `try_first_pass` - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password.
- `retry=3` - Allow 3 tries before sending back a failure.
- `minlen=14` - password must be 14 characters or more

**** Either of the following can be used to enforce complex passwords:****

- `minclass=4` - provide at least four classes of characters for the new password

Or

- `dcredit=-1` - provide at least one digit
- `ucredit=-1` - provide at least one uppercase character
- `ocredit=-1` - provide at least one special character
- `lcredit=-1` - provide at least one lowercase character

The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies

Rationale:

Strong passwords protect systems from being hacked through brute force methods.

Audit:

Verify password creation requirements conform to organization policy:

Run the following command and verify that retry conforms to organization policy.

```
# grep pam_pwquality.so /etc/pam.d/system-auth /etc/pam.d/password-auth
```

Output should be similar to:

```
/etc/pam.d/system-auth:password requisite pam_pwquality.so try_first_pass  
local_users_only enforce-for-root retry=3  
/etc/pam.d/password-auth:password requisite pam_pwquality.so try_first_pass  
local_users_only enforce-for-root retry=3
```

Run the following commands and verify password length requirements conform to organization policy.

```
# grep ^minlen /etc/security/pwquality.conf
```

Verify minlen is 14 or more

Run one of the following commands and verify that password complexity conforms to organization policy.

```
# grep ^minclass /etc/security/pwquality.conf
```

Or

```
# grep -E "^\s*\$credit\s*=" /etc/security/pwquality.conf
```

Remediation:

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password length to conform to site policy

```
minlen = 14
```

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password complexity to conform to site policy

```
minclass = 4
```

Or

```
dcredit = -1  
ucredit = -1  
ocredit = -1  
lcredit = -1
```

Run the following to update the system-auth and password-auth files

```
CP=$(authselect current | awk 'NR == 1 {print $3}' | grep custom/)  
for FN in system-auth password-auth; do  
    [[ -n $CP ]] && PTF=/etc/authselect/$CP/$FN || PTF=/etc/authselect/$FN  
    [[ -z $(grep -E  
'^\s*password\s+requisite\s+pam_pwquality.so\s+.*enforce-for-root\s*.*$'  
$PTF) ]] && sed -ri  
's/^(\s*(password\s+requisite\s+pam_pwquality.so\s+)(.*))$/\1\2 enforce-for-  
root/' $PTF  
    [[ -n $(grep -E  
'^\s*password\s+requisite\s+pam_pwquality.so\s+.*\s+retry=\S+\s*.*$' $PTF) ]]  
&& sed -ri '/pwquality/s/retry=\S+/retry=3/' $PTF || sed -ri  
's/^(\s*(password\s+requisite\s+pam_pwquality.so\s+)(.*))$/\1\2 retry=3/' $PTF  
done  
authselect apply-changes
```

Additional Information:

all default authselect profiles have pam_pwquality enabled with the expectation that options will be specified in pwquality.conf

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	●	●	●

5.4.2 Ensure the system locks an account after three unsuccessful logon attempts (Automated)

Profile Applicability:

- STIG

Description:

The operating system must automatically lock an account when three unsuccessful logon attempts occur.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Check that the system locks an account after three unsuccessful logon attempts with the following commands:

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

Note: This check applies to RHEL versions 8.0 and 8.1, if the system is RHEL version 8.2 or newer, this check is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "deny" option is not set to "3" or less (but not "0") on the "preauth" line with the "pam_faillock.so" module, or is missing from this line, this is a finding.

If any line referencing the "pam_faillock.so" module is commented out, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "deny" option is not set to "3" or less (but not "0") on the "preauth" line with the "pam_faillock.so" module, or is missing from this line, this is a finding.

If any line referencing the "pam_faillock.so" module is commented out, this is a finding.

Remediation:

Configure the operating system to lock an account when three unsuccessful logon attempts occur.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230332

Rule ID: SV-230332r627750_rule

STIG ID: RHEL-08-020010

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

5.4.3 Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts within 15 minutes (Automated)

Profile Applicability:

- STIG

Description:

The operating system must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam_faillock.so module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be re-enabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts within 15 minutes:

```
# grep 'fail_interval =' /etc/security/faillock.conf  
fail_interval = 900
```

If the "fail_interval" option is not set to "900" or more, is missing or commented out, this is a finding.

Remediation:

Configure the operating system to lock an account when three unsuccessful logon attempts occur in 15 minutes.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
fail_interval = 900
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230335

Rule ID: SV-230335r743969_rule

STIG ID: RHEL-08-020013

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

5.4.4 Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes (Automated)

Profile Applicability:

- STIG

Description:

The operating system must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program. From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Check that the system locks an account after three unsuccessful logon attempts within a period of 15 minutes with the following commands:

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

Note: This check applies to RHEL versions 8.0 and 8.1, if the system is RHEL version 8.2 or newer, this check is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "fail_interval" option is not set to "900" or less (but not "0") on the "preauth" lines with the "pam_faillock.so" module, or is missing from this line, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "fail_interval" option is not set to "900" or less (but not "0") on the "preauth" lines with the "pam_faillock.so" module, or is missing from this line, this is a finding.

Remediation:

Configure the operating system to lock an account when three unsuccessful logon attempts occur in 15 minutes.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230334

Rule ID: SV-230334r627750_rule

STIG ID: RHEL-08-020012

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

5.4.5 Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts (Automated)

Profile Applicability:

- STIG

Description:

The operating system must automatically lock an account when three unsuccessful logon attempts occur.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam_faillock.so module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts:

```
# grep 'deny =' /etc/security/faillock.conf
deny = 3
```

If the "deny" option is not set to "3" or less (but not "0"), is missing or commented out, this is a finding.

Remediation:

Configure the operating system to lock an account when three unsuccessful logon attempts occur.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
deny = 3
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230333

Rule ID: SV-230333r743966_rule

STIG ID: RHEL-08-020011

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

5.4.6 Ensure lockout for failed password attempts is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Lock out users after n unsuccessful consecutive login attempts.

- `deny=` - Number of attempts before the account is locked
- `unlock_time=` - Time in seconds before the account is unlocked

Set the lockout number and unlock time to follow local site policy.

Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Audit:

Verify password lockouts are configured. These settings are commonly configured with the `pam_tally2.so` and `pam_faillock.so` modules found in `/etc/pam.d/common-auth` or `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth`.

Examples:

Run the following command and review the output to ensure that it follows local site policy. `deny` should be no greater than 5 and `unlock_time` should be no less than 900 seconds

```
# grep -E '^s*auth\s+required\s+pam_faillock.so\s+' /etc/pam.d/password-auth  
/etc/pam.d/system-auth
```

Output should look similar to:

<code>/etc/pam.d/password-auth:auth deny=5 unlock_time=900</code>	<code>required</code>	<code>pam_faillock.so preauth silent</code>
<code>/etc/pam.d/password-auth:auth deny=5 unlock_time=900</code>	<code>required</code>	<code>pam_faillock.so authfail</code>
<code>/etc/pam.d/system-auth:auth deny=5 unlock_time=900</code>	<code>required</code>	<code>pam_faillock.so preauth silent</code>
<code>/etc/pam.d/system-auth:auth deny=5 unlock_time=900</code>	<code>required</code>	<code>pam_faillock.so authfail</code>

Remediation:

Set password lockouts and unlock times to conform to site policy

Run the following to update the `system-auth` and `password-auth` files. This script will update/add the `deny=5` and `unlock_time=900` options.

This script should be modified as needed to follow local site policy.

```
CP=$(authselect current | awk 'NR == 1 {print $3}' | grep custom)
for FN in system-auth password-auth; do
    [[ -n $CP ]] && PTF=/etc/authselect/$CP/$FN || PTF=/etc/authselect/$FN
    [[ -n $(grep -E
'^\s*auth\s+required\s+pam_faillock.so\s+.*deny=\S+\s*.*$' $PTF) ]] && sed -ri '/pam_faillock.so/s/deny=\S+/deny=5/g' $PTF || sed -ri 's/^(\s*(auth\s+required\s+pam_faillock\.so\s+)(.*[^{}])(\{.*\})|)\$/\1\2
deny=5 \3/' $PTF
    [[ -n $(grep -E
'^\s*auth\s+required\s+pam_faillock.so\s+.*unlock_time=\S+\s*.*$' $PTF) ]] && sed -ri '/pam_faillock.so/s/unlock_time=\S+/unlock_time=900/g' $PTF || sed -ri 's/^(\s*(auth\s+required\s+pam_faillock\.so\s+)(.*[^{}])(\{.*\})|)\$/\1\2
unlock_time=900 \3/' $PTF
done
authselect apply-changes
```

Additional Information:

Additional module options may be set, recommendation only covers those listed here. If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_faillock.so` module, the user can be unlocked by issuing the command `faillock -u --reset`. This command sets the failed count to 0, effectively unlocking the user.

Use of the "audit" keyword may log credentials in the case of user error during authentication. This risk should be evaluated in the context of the site policies of your organization.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

5.4.7 Ensure password reuse is limited (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/security/opasswd` file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

- `remember=<5>` - Number of old passwords to remember

Rationale:

Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password.

Note: These change only apply to accounts configured on the local system.

Audit:

Run the following command and verify that the remembered password history is 5 or more.

```
# grep -P '^h*password\h+(requisite|sufficient)\h+(pam_pwhistory\.so|pam_unix\.so)\h+([^\#\n\r]+)\h+)?remember=([5-9]|1-9][0-9]+)\h*(\h+.*)?$$' /etc/pam.d/system-auth
```

The output should be similar to:

```
password      requisite      pam_pwhistory.so try_first_pass local_users_only
enforce-for-root retry=3 remember=5
password      sufficient     pam_unix.so sha512 shadow  try_first_pass
use_authtok  remember=5
```

Remediation:

Set remembered password history to conform to site policy.

Run the following script to add or modify the `pam_pwhistory.so` and `pam_unix.so` lines to include the `remember` option:

```
#!/bin/bash

if authselect current | awk 'NR == 1 {print $3}' | grep -q custom/; then
    PTF=/etc/authselect/"$(authselect current | awk 'NR == 1 {print $3}' | grep custom)"/system-auth
else
    PTF=/etc/authselect/system-auth
fi

if grep -Eq
'^\s*password\s+(sufficient\s+pam_unix|requi(red|site)\s+pam_pwhistory)\.so\s+([^\#]+\s+)\*remember=\$+\s*\.*\$' $PTF; then
    sed -ri
's/^(\s*(password\s+(requisite|sufficient)\s+(pam_pwhistory\.so|pam_unix\.so)\s+)\.(.*)(remember=\$+\s*)\.(.*))$/\1\4 remember=5 \6/' $PTF
else
    sed -ri
's/^(\s*(password\s+(requisite|sufficient)\s+(pam_pwhistory\.so|pam_unix\.so)\s+)\.(.*))$/\1\4 remember=5/' $PTF
fi

authselect apply-changes
```

Additional Information:

Additional module options may be set, recommendation only covers those listed here.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

5.4.8 Ensure password hashing algorithm is SHA-512 (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The commands below change password encryption from `md5` to `sha512` (a much stronger hashing algorithm). All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.

Rationale:

The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

Note that these changes only apply to accounts configured on the local system.

Audit:

Verify password hashing algorithm is `sha512`. This setting is configured with the `pam_unix.so sha512` option found in `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth`

Run the following command:

```
# grep -E '^s*password\s+sufficient\s+pam_unix.so\s+.*sha512\s*.*$'  
/etc/pam.d/password-auth /etc/pam.d/system-auth
```

The output should be similar to:

```
/etc/pam.d/password-auth:password      sufficient      pam_unix.so sha512  
shadow  try_first_pass use_authok  
/etc/pam.d/system-auth:password      sufficient      pam_unix.so sha512  
shadow  try_first_pass use_authok remember=5
```

Remediation:

Set password hashing algorithm to sha512.

Run the following script to dd or modify the pam_unix.so lines in the password-auth and system-auth files to include the sha512 option:

```
CP=$(authselect current | awk 'NR == 1 {print $3}' | grep custom/)  
for FN in system-auth password-auth; do  
    [ -z $(grep -E  
        '^\\s*password\\s+sufficient\\s+pam_unix.so\\s+.*sha512\\s*.*$' $PTF) ] ] && sed -  
    ri 's/^\\s*(password\\s+sufficient\\s+pam_unix.so\\s+)(.*)$/\\1\\2 sha512/' $PTF  
done  
authselect apply-changes
```

Additional Information:

Additional module options may be set, recommendation only covers those listed here. If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login. To accomplish that, the following commands can be used.

Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# awk -F: '($3<"$(awk '/^\\s*UID_MIN/{print $2}' /etc/login.defs)" && $1 !=  
"nfsnobody") { print $1 }' /etc/passwd | xargs -n 1 chage -d 0
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

5.4.9 Ensure a minimum number of hash rounds is configured (Automated)

Profile Applicability:

- STIG

Description:

The system-auth file must be configured to use a sufficient number of hashing rounds.

Rationale:

The system must use a strong hashing algorithm to store the password. The system must use a sufficient number of hashing rounds to ensure the required level of entropy.

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Audit:

Check that a minimum number of hash rounds is configured by running the following command:

```
# grep rounds /etc/pam.d/system-auth
password sufficient pam_unix.so sha512 rounds=5000
```

If "rounds" has a value below "5000", or is commented out, this is a finding.

Remediation:

Configure the operating system to encrypt all stored passwords with a strong cryptographic hash.

Edit/modify the following line in the "etc/pam.d/system-auth" file and set "rounds" to a value no lower than "5000":

```
password sufficient pam_unix.so sha512 rounds=5000
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244520

Rule ID: SV-244520r743809_rule

STIG ID: RHEL-08-010131

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.4.10 Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes until released by an administrator (Automated)

Profile Applicability:

- STIG

Description:

The operating system must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Check that the system locks an account after three unsuccessful logon attempts within a period of 15 minutes until released by an administrator with the following commands:

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

Note: This check applies to RHEL versions 8.0 and 8.1, if the system is RHEL version 8.2 or newer, this check is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "unlock_time" option is not set to "0" on the "preauth" and "authfail" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "unlock_time" option is not set to "0" on the "preauth" and "authfail" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

Remediation:

Configure the operating system to lock an account until released by an administrator when three unsuccessful logon attempts occur in 15 minutes.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230336

Rule ID: SV-230336r627750_rule

STIG ID: RHEL-08-020014

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

5.4.11 Ensure the "/etc/security/faillock.conf" file is configured to lock an account until released by an administrator after three unsuccessful logon attempts (Automated)

Profile Applicability:

- STIG

Description:

The operating system must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam_faillock.so module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to lock an account until released by an administrator after three unsuccessful logon attempts:

```
# grep 'unlock_time =' /etc/security/faillock.conf
unlock_time = 0
```

If the "unlock_time" option is not set to "0", is missing or commented out, this is a finding.

Remediation:

Configure the operating system to lock an account until released by an administrator when three unsuccessful logon attempts occur in 15 minutes.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
unlock_time = 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230337

Rule ID: SV-230337r743972_rule

STIG ID: RHEL-08-020015

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

5.4.12 Ensure the faillock directory contents persist after a reboot (Automated)

Profile Applicability:

- STIG

Description:

The operating system must ensure account lockouts persist.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Check that the faillock directory contents persists after a reboot with the following commands:

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

Note: This check applies to RHEL versions 8.0 and 8.1, if the system is RHEL version 8.2 or newer, this check is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "dir" option is not set to a non-default documented tally log directory on the "preauth" and "authfail" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "dir" option is not set to a non-default documented tally log directory on the "preauth" and "authfail" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

Remediation:

Configure the operating system to maintain the contents of the faillock directory after a reboot.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

Note: Using the default faillock directory of /var/run/faillock will result in the contents being cleared in the event of a reboot.

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230338

Rule ID: SV-230338r627750_rule

STIG ID: RHEL-08-020016

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.4.13 Ensure the "/etc/security/faillock.conf" file is configured to use a non-default faillock directory to ensure contents persist after reboot (Automated)

Profile Applicability:

- STIG

Description:

The operating system must ensure account lockouts persist.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam_faillock.so module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to RHEL versions 8.2 or newer. If the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured use a non-default faillock directory to ensure contents persist after reboot:

```
# grep 'dir =' /etc/security/faillock.conf
dir = /var/log/faillock
```

If the "dir" option is not set to a non-default documented tally log directory, is missing or commented out, this is a finding.

Remediation:

Configure the operating system to maintain the contents of the faillock directory after a reboot.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
dir = /var/log/faillock
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230339

Rule ID: SV-230339r743975_rule

STIG ID: RHEL-08-020017

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.4.14 Ensure the system prevents informative messages to the user about logon information (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent system messages from being presented when three unsuccessful logon attempts occur.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Check that the system prevents informative messages from being presented to the user pertaining to logon information with the following commands:

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

Note: This check applies to RHEL versions 8.0 and 8.1, if the system is RHEL version 8.2 or newer, this check is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "silent" option is missing from the "preauth" line with the "pam_faillock.so" module, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "silent" option is missing from the "preauth" line with the "pam_faillock.so" module, this is a finding.

Remediation:

Configure the operating system to prevent informative messages from being presented at logon attempts.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230340

Rule ID: SV-230340r627750_rule

STIG ID: RHEL-08-020018

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.4.15 Ensure the "/etc/security/faillock.conf" file is configured to prevent informative messages about logon attempts (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent system messages from being presented when three unsuccessful logon attempts occur.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam_faillock.so module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to prevent informative messages from being presented at logon attempts:

```
# grep silent /etc/security/faillock.conf  
silent
```

If the "silent" option is not set, is missing or commented out, this is a finding.

Remediation:

Configure the operating system to prevent informative messages from being presented at logon attempts.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
silent
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230341

Rule ID: SV-230341r743978_rule

STIG ID: RHEL-08-020019

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.4.16 Ensure the system logs user name information when unsuccessful logon attempts occur (Automated)

Profile Applicability:

- STIG

Description:

The operating system must log user name information when unsuccessful logon attempts occur.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

The "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the "pam_faillock.so" module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Check that the system logs user name information when unsuccessful logon attempts occur with the following commands:

If the system is RHEL version 8.2 or newer, this check is not applicable.

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth  
  
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit  
deny=3 even_root fail_interval=900 unlock_time=0  
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0  
account required pam_faillock.so
```

If the "audit" option is missing from the "preauth" line with the "pam_faillock.so" module, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth  
  
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit  
deny=3 even_root fail_interval=900 unlock_time=0  
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0  
account required pam_faillock.so
```

If the "audit" option is missing from the "preauth" line with the "pam_faillock.so" module, this is a finding.

Remediation:

Configure the operating system to log user name information when unsuccessful logon attempts occur.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit  
deny=3 even_root fail_interval=900 unlock_time=0  
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0  
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230342

Rule ID: SV-230342r646872_rule

STIG ID: RHEL-08-020020

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

5.4.17 Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur (Automated)

Profile Applicability:

- STIG

Description:

The operating system must log user name information when unsuccessful logon attempts occur.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam_faillock.so module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur:

```
# grep audit /etc/security/faillock.conf  
audit
```

If the "audit" option is not set, is missing or commented out, this is a finding.

Remediation:

Configure the operating system to log user name information when unsuccessful logon attempts occur.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
audit
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230343

Rule ID: SV-230343r743981_rule

STIG ID: RHEL-08-020021

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

5.4.18 Ensure the system includes the root account when locking an account after three unsuccessful logon attempts within a period of 15 minutes (Automated)

Profile Applicability:

- STIG

Description:

The operating system must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

The "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the "pam_faillock.so" module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Check that the system includes the root account when locking an account after three unsuccessful logon attempts within a period of 15 minutes with the following commands:
If the system is RHEL version 8.2 or newer, this check is not applicable.

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth  
  
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit  
deny=3 even_deny_root fail_interval=900 unlock_time=0  
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0  
account required pam_faillock.so
```

If the "even_deny_root" option is missing from the "preauth" line with the "pam_faillock.so" module, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth  
  
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit  
deny=3 even_deny_root fail_interval=900 unlock_time=0  
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0  
account required pam_faillock.so
```

If the "even_deny_root" option is missing from the "preauth" line with the "pam_faillock.so" module, this is a finding.

Remediation:

Configure the operating system to include root when locking an account after three unsuccessful logon attempts occur in 15 minutes.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit  
deny=3 even_deny_root fail_interval=900 unlock_time=0  
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0  
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230344

Rule ID: SV-230344r646874_rule

STIG ID: RHEL-08-020022

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	●	●	●

5.4.19 Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur (Automated)

Profile Applicability:

- STIG

Description:

The operating system must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam_faillock.so module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From the "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be re-enabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur:

```
# grep even_deny_root /etc/security/faillock.conf
even_deny_root
```

If the "even_deny_root" option is not set, is missing or commented out, this is a finding.

Remediation:

Configure the operating system to include root when locking an account after three unsuccessful logon attempts occur in 15 minutes.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
even_deny_root
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230345

Rule ID: SV-230345r743984_rule

STIG ID: RHEL-08-020023

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

5.4.20 Ensure the operating system prohibits password reuse for a minimum of five generations (Automated)

Profile Applicability:

- STIG

Description:

Passwords must be prohibited from reuse for a minimum of five generations.

Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to reuse their password consecutively when that password has exceeded its defined lifetime, the end result is a password that is not changed per policy requirements.

RHEL 8 operating system's utilize "pwquality" consecutively as a mechanism to enforce password complexity. This is set in both: /etc/pam.d/password-auth /etc/pam.d/system-auth.

Note that manual changes to the listed files may be overwritten by the "authselect" program.

Audit:

Verify the operating system prohibits password reuse for a minimum of five generations.

Check for the value of the "remember" argument in "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" with the following command:

```
# grep -i remember /etc/pam.d/system-auth /etc/pam.d/password-auth  
password required pam_pwhistory.so use_authtok remember=5 retry=3
```

If the line containing "pam_pwhistory.so" does not have the "remember" module argument set, is commented out, or the value of the "remember" module argument is set to less than "5", this is a finding.

Remediation:

Configure the operating system to prohibit password reuse for a minimum of five generations.

Add the following line in "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" (or modify the line to have the required value):

```
password required pam_pwhistory.so use_authtok remember=5 retry=3
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230368

Rule ID: SV-230368r627750_rule

STIG ID: RHEL-08-020220

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

5.4.21 Ensure the operating system uses multifactor authentication for local access to accounts (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement smart card logon for multifactor authentication for access to interactive accounts.

Rationale:

Using an authentication device, such as a Common Access Card (CAC) or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD CAC.

There are various methods of implementing multifactor authentication for RHEL 8. Some methods include a local system multifactor account mapping or joining the system to a domain and utilizing a Red Hat idM server or Microsoft Windows Active Directory server. Any of these methods will require that the client operating system handle the multifactor authentication correctly.

Satisfies: SRG-OS-000105-GPOS-00052, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055

Audit:

Verify the operating system uses multifactor authentication for local access to accounts.

Note: If the System Administrator demonstrates the use of an approved alternate multifactor authentication method, this requirement is not applicable.

Check that the "pam_cert_auth" setting is set to "true" in the "/etc/sssd/sssd.conf" file.

Check that the "try_cert_auth" or "require_cert_auth" options are configured in both "/etc/pam.d/system-auth" and "/etc/pam.d/smardcard-auth" files with the following command:

```
# grep cert_auth /etc/sssd/sssd.conf /etc/pam.d/*
/etc/sssd/sssd.conf:pam_cert_auth = True
/etc/pam.d/smardcard-auth:auth sufficient pam_sss.so try_cert_auth
/etc/pam.d/system-auth:auth [success=done authinfo_unavail=ignore
ignore=ignore default=die] pam_sss.so try_cert_auth
```

If "pam_cert_auth" is not set to "true" in "/etc/sssd/sssd.conf", this is a finding.

If "pam_sss.so" is not set to "try_cert_auth" or "require_cert_auth" in both the "/etc/pam.d/smardcard-auth" and "/etc/pam.d/system-auth" files, this is a finding.

Remediation:

Configure the operating system to use multifactor authentication for local access to accounts.

Add or update the "pam_cert_auth" setting in the "/etc/sssd/sssd.conf" file to match the following line:

```
[pam]
pam_cert_auth = True
```

Add or update "pam_sss.so" with "try_cert_auth" or "require_cert_auth" in the "/etc/pam.d/system-auth" and "/etc/pam.d/smardcard-auth" files based on the following examples:

```
/etc/pam.d/smardcard-auth:auth sufficient pam_sss.so try_cert_auth
/etc/pam.d/system-auth:auth [success=done authinfo_unavail=ignore
ignore=ignore default=die] pam_sss.so try_cert_auth
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230372

Rule ID: SV-230372r627750_rule

STIG ID: RHEL-08-020250

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.	●	●	●

5.4.22 Ensure the date and time of the last successful account logon upon logon is displayed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must display the date and time of the last successful account logon upon logon.

Rationale:

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Audit:

Verify users are provided with feedback on when account accesses last occurred with the following command:

```
# grep pam_lastlog /etc/pam.d/postlogin  
session required pam_lastlog.so showfailed
```

If "pam_lastlog" is missing from "/etc/pam.d/postlogin" file, or the silent option is present, this is a finding.

Remediation:

Configure the operating system to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/postlogin".

Add the following line to the top of "/etc/pam.d/postlogin":

```
session required pam_lastlog.so showfailed
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230381

Rule ID: SV-230381r627750_rule

STIG ID: RHEL-08-020340

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.4.23 Ensure the "pam_unix.so" module is configured to use sha512 (Automated)

Profile Applicability:

- STIG

Description:

The pam_unix.so module must be configured in the system-auth file to use a FIPS 140-2 approved cryptographic hashing algorithm for system authentication.

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

RHEL 8 operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

Audit:

Verify that the "pam_unix.so" module is configured to use sha512.

Check that the "pam_unix.so" module is configured to use sha512 in "/etc/pam.d/system-auth" with the following command:

```
# grep password /etc/pam.d/system-auth | grep pam_unix  
password sufficient pam_unix.so sha512 rounds=5000
```

If "sha512" is missing, or is commented out, this is a finding.

Remediation:

Configure the operating system to use a FIPS 140-2 approved cryptographic hashing algorithm for system authentication.

Edit/modify the following line in the "/etc/pam.d/system-auth" file to include the sha512 option for "pam_unix.so":

```
password sufficient pam_unix.so sha512 rounds=5000
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244524

Rule ID: SV-244524r743821_rule

STIG ID: RHEL-08-010159

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

5.4.24 Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/system-auth" file (Automated)

Profile Applicability:

- STIG

Description:

The operating system must configure the use of the "pam_faillock.so" module in the "/etc/pam.d/system-auth" file.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the "pam_faillock.so" module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

The preauth argument must be used when the module is called before the modules which ask for the user credentials such as the password.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "pam_faillock.so" module is present in the "/etc/pam.d/system-auth" file:

```
# grep pam_faillock.so /etc/pam.d/system-auth
auth required pam_faillock.so preauth
auth required pam_faillock.so authfail
account required pam_faillock.so
```

If the pam_faillock.so module is not present in the "/etc/pam.d/system-auth" file with the "preauth" line listed before "pam_unix.so", this is a finding.

Remediation:

Configure the operating system to include the use of the "pam_faillock.so" module in the "/etc/pam.d/system-auth" file.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" file to match the following lines:

Note: The "pcreauth" line must be listed before "pam_unix.so".

```
auth required pam_faillock.so preauth  
auth required pam_faillock.so authfail  
account required pam_faillock.so
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244533

Rule ID: SV-244533r743848_rule

STIG ID: RHEL-08-020025

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.4.25 Ensure blank or null passwords in the "system-auth" file cannot be used (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not allow blank or null passwords in the "system-auth" file.

Rationale:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Audit:

To verify that null passwords cannot be used, run the following command:

```
# grep -i nullok /etc/pam.d/system-auth
```

If output is produced, this is a finding.

Remediation:

Remove any instances of the "nullok" option in the "/etc/pam.d/system-auth" file to prevent logons with empty passwords.

Note: Manual changes to the listed file may be overwritten by the "authselect" program.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244540

Rule ID: SV-244540r743869_rule

STIG ID: RHEL-08-020331

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

5.4.26 Ensure blank or null passwords in the "password-auth" file cannot be used (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not allow blank or null passwords in the "password-auth" file.

Rationale:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Audit:

To verify that null passwords cannot be used, run the following command:

```
# grep -i nullok /etc/pam.d/password-auth
```

If output is produced, this is a finding.

Remediation:

Remove any instances of the "nullok" option in the "/etc/pam.d/password-auth" file to prevent logons with empty passwords.

Note: Manual changes to the listed file may be overwritten by the "authselect" program.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244541

Rule ID: SV-244541r743872_rule

STIG ID: RHEL-08-020332

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

5.4.27 Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/password-auth" file (Automated)

Profile Applicability:

- STIG

Description:

The operating system must configure the use of the "pam_faillock.so" module in the "/etc/pam.d/password-auth" file.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the "pam_faillock.so" module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

The preauth argument must be used when the module is called before the modules which ask for the user credentials such as the password.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "pam_faillock.so" module is present in the "/etc/pam.d/password-auth" file:

```
# grep pam_faillock.so /etc/pam.d/password-auth
auth required pam_faillock.so preauth
auth required pam_faillock.so authfail
account required pam_faillock.so
```

If the "pam_faillock.so" module is not present in the "/etc/pam.d/password-auth" file with the "preauth" line listed before "pam_unix.so", this is a finding.

Remediation:

Configure the operating system to include the use of the "pam_faillock.so" module in the "/etc/pam.d/password-auth" file.

Add/Modify the appropriate sections of the "/etc/pam.d/password-auth" file to match the following lines:

Note: The "pcreauth" line must be listed before "pam_unix.so".

```
auth required pam_faillock.so preauth
auth required pam_faillock.so authfail
account required pam_faillock.so
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244534

Rule ID: SV-244534r743851_rule

STIG ID: RHEL-08-020026

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.5 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

5.5.1 Set Shadow Password Suite Parameters

While a majority of the password control parameters have been moved to PAM, some parameters are still available through the shadow password suite. Any changes made to `/etc/login.defs` will only be applied if the `usermod` command is used. If user IDs are added a different way, use the `chage` command to effect changes to individual user IDs.

5.5.1.1 Ensure password expiration is 365 days or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PASS_MAX_DAYS` parameter in `/etc/login.defs` allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the `PASS_MAX_DAYS` parameter be set to less than or equal to 365 days.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Audit:

Run the following command and verify `PASS_MAX_DAYS` conforms to site policy (no more than 365 days):

```
# grep PASS_MAX_DAYS /etc/login.defs  
PASS_MAX_DAYS 365
```

Run the following command and Review list of users and `PASS_MAX_DAYS` to verify that all users' `PASS_MAX_DAYS` conforms to site policy (no more than 365 days):

```
# grep -E '^[:]+:[^!*]' /etc/shadow | cut -d: -f1,5  
<user>:<PASS_MAX_DAYS>
```

Remediation:

Set the `PASS_MAX_DAYS` parameter to conform to site policy in `/etc/login.defs`:

```
PASS_MAX_DAYS 365
```

Modify user parameters for all users with a password set to match:

```
# chage --maxdays 365 <user>
```

Additional Information:

You can also check this setting in `/etc/shadow` directly. The 5th field should be 365 or less for all users with a password.

Note: A value of -1 will disable password expiration. Additionally, the password expiration must be greater than the minimum days between password changes or users will be unable to change their password.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	●	●	●

5.5.1.2 Ensure the shadow password suite configuration is set to encrypt password with a FIPS 140-2 approved cryptographic hashing algorithm. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must encrypt all stored passwords with a FIPS 140-2 approved cryptographic hashing algorithm.

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements.

Audit:

Verify that the shadow password suite configuration is set to encrypt password with a FIPS 140-2 approved cryptographic hashing algorithm.

Check the hashing algorithm that is being used to hash passwords with the following command:

```
# grep -i crypt /etc/login.defs  
ENCRYPT_METHOD SHA512
```

If "ENCRYPT_METHOD" does not equal SHA512 or greater, this is a finding.

Remediation:

Configure the operating system to encrypt all stored passwords.

Edit/Modify the following line in the "/etc/login.defs" file and set "[ENCRYPT_METHOD]" to SHA512.

```
ENCRYPT_METHOD SHA512
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230231

Rule ID: SV-230231r627750_rule

STIG ID: RHEL-08-010110

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

5.5.1.3 Ensure the value of the "maxrepeat" option in "/etc/security/pwquality.conf" is "3" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must require the maximum number of repeating characters be limited to three when passwords are changed.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize "pwquality" as a mechanism to enforce password complexity. The "maxrepeat" option sets the maximum number of allowed same consecutive characters in a new password.

Audit:

Check for the value of the "maxrepeat" option in "/etc/security/pwquality.conf" with the following command:

```
# grep maxrepeat /etc/security/pwquality.conf  
maxrepeat = 3
```

If the value of "maxrepeat" is set to more than "3" or is commented out, this is a finding.

Remediation:

Configure the operating system to require the change of the number of repeating consecutive characters when passwords are changed by setting the "maxrepeat" option.

Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
maxrepeat = 3
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230361

Rule ID: SV-230361r627750_rule

STIG ID: RHEL-08-020150

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.4 Ensure the value of the "difok" option in "/etc/security/pwquality.conf" is "8" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must require the change of at least 8 characters when passwords are changed.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize "pwquality" as a mechanism to enforce password complexity. The "difok" option sets the number of characters in a password that must not be present in the old password.

Audit:

Verify the value of the "difok" option in "/etc/security/pwquality.conf" with the following command:

```
# grep difok /etc/security/pwquality.conf  
difok = 8
```

If the value of "difok" is set to less than "8" or is commented out, this is a finding.

Remediation:

Configure the operating system to require the change of at least eight of the total number of characters when passwords are changed by setting the "difok" option.

Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
difok = 8
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230363

Rule ID: SV-230363r627750_rule

STIG ID: RHEL-08-020170

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.5 Ensure the value of the "minclass" option in "/etc/security/pwquality.conf" is "4" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must require the change of at least four character classes when passwords are changed.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating system utilize "pwquality" as a mechanism to enforce password complexity. The "minclass" option sets the minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others).

Audit:

Verify the value of the "minclass" option in "/etc/security/pwquality.conf" with the following command:

```
# grep minclass /etc/security/pwquality.conf  
minclass = 4
```

If the value of "minclass" is set to less than "4" or is commented out, this is a finding.

Remediation:

Configure the operating system to require the change of at least four character classes when passwords are changed by setting the "minclass" option.

Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
minclass = 4
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230362

Rule ID: SV-230362r627750_rule

STIG ID: RHEL-08-020160

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.6 Ensure the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" is "4" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must require the maximum number of repeating characters of the same character class be limited to four when passwords are changed.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize "pwquality" as a mechanism to enforce password complexity. The "maxclassrepeat" option sets the maximum number of allowed same consecutive characters in the same class in the new password.

Audit:

Check for the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" with the following command:

```
# grep maxclassrepeat /etc/security/pwquality.conf  
maxclassrepeat = 4
```

If the value of "maxclassrepeat" is set to more than "4" or is commented out, this is a finding.

Remediation:

Configure the operating system to require the change of the number of repeating characters of the same character class when passwords are changed by setting the "maxclassrepeat" option.

Add the following line to "/etc/security/pwquality.conf" conf (or modify the line to have the required value):

```
maxclassrepeat = 4
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230360

Rule ID: SV-230360r627750_rule

STIG ID: RHEL-08-020140

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.7 Ensure the value for "dcredit" in "/etc/security/pwquality.conf" is "-1" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enforce password complexity by requiring that at least one numeric character be used.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize "pwquality" as a mechanism to enforce password complexity. Note that in order to require numeric characters, without degrading the minlen value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

Audit:

Verify the value for "dcredit" in "/etc/security/pwquality.conf" with the following command:

```
# grep dcredit /etc/security/pwquality.conf  
dcredit = -1
```

If the value of "dcredit" is a positive number or is commented out, this is a finding.

Remediation:

Configure the operating system to enforce password complexity by requiring that at least one numeric character be used by setting the "dcredit" option.

Add the following line to /etc/security/pwquality.conf (or modify the line to have the required value):

```
dcredit = -1
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230359

Rule ID: SV-230359r627750_rule

STIG ID: RHEL-08-020130

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.8 Ensure the value for "lcredit" in "/etc/security/pwquality.conf" is "-1" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enforce password complexity by requiring that at least one lower-case character be used.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize pwquality as a mechanism to enforce password complexity. Note that in order to require lower-case characters without degrading the "minlen" value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

Audit:

Verify the value for "lcredit" in "/etc/security/pwquality.conf" with the following command:

```
# grep lcredit /etc/security/pwquality.conf  
lcredit = -1
```

If the value of "lcredit" is a positive number or is commented out, this is a finding.

Remediation:

Configure the operating system to enforce password complexity by requiring that at least one lower-case character be used by setting the "lcredit" option.

Add the following line to /etc/security/pwquality.conf (or modify the line to have the required value):

```
lcredit = -1
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230358

Rule ID: SV-230358r627750_rule

STIG ID: RHEL-08-020120

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.9 Ensure the value for "ucredit" in "/etc/security/pwquality.conf" is "-1" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enforce password complexity by requiring that at least one uppercase character be used.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize pwquality as a mechanism to enforce password complexity. Note that in order to require uppercase characters, without degrading the "minlen" value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

Audit:

Verify the value for "ucredit" in "/etc/security/pwquality.conf" with the following command:

```
# grep ucredit /etc/security/pwquality.conf  
ucredit = -1
```

If the value of "ucredit" is a positive number or is commented out, this is a finding.

Remediation:

Configure the operating system to enforce password complexity by requiring that at least one uppercase character be used by setting the "ucredit" option.

Add the following line to /etc/security/pwquality.conf (or modify the line to have the required value):

```
ucredit = -1
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230357

Rule ID: SV-230357r627750_rule

STIG ID: RHEL-08-020110

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.10 Ensure the operating system uses "pwquality" to enforce the password complexity rules (Automated)

Profile Applicability:

- STIG

Description:

The operating system must ensure a password complexity module is enabled.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

RHEL 8 operating systems utilize "pwquality" as a mechanism to enforce password complexity. This is set in both: /etc/pam.d/password-auth /etc/pam.d/system-auth
Note the value of "retry" set in these configuration files should be between "1" and "3".
Manual changes to the listed files may be overwritten by the "authselect" program.

Audit:

Verify the operating system uses "pwquality" to enforce the password complexity rules.
Check for the use of "pwquality" with the following commands:

```
# cat /etc/pam.d/password-auth | grep pam_pwquality
password required pam_pwquality.so retry=3

# cat /etc/pam.d/system-auth | grep pam_pwquality
password required pam_pwquality.so retry=3
```

If both commands do not return a line containing the value "pam_pwquality.so", or the line is commented out, this is a finding.

If the value of "retry" is set to "0" or greater than "3", this is a finding.

Remediation:

Configure the operating system to use "pwquality" to enforce password complexity rules.

Add the following line to both "/etc/pam.d/password-auth" and "/etc/pam.d/system-auth" (or modify the line to have the required value):

```
password required pam_pwquality.so retry=3
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230356

Rule ID: SV-230356r627750_rule

STIG ID: RHEL-08-020100

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

5.5.1.11 Ensure minimum days between password changes is 7 or more (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PASS_MIN_DAYS` parameter in `/etc/login.defs` allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that `PASS_MIN_DAYS` parameter be set to 7 or more days.

Rationale:

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Audit:

Run the following command and verify `PASS_MIN_DAYS` conforms to site policy (no less than 7 days):

```
# grep ^\s*PASS_MIN_DAYS /etc/login.defs  
PASS_MIN_DAYS 7
```

Run the following command and Review list of users and `PASS_MIN_DAYS` to Verify that all users' `PASS_MIN_DAYS` conform s to site policy (no less than 7 days):

```
# grep -E ^[^:]+:[^\\!*] /etc/shadow | cut -d: -f1,4  
<user>:<PASS_MIN_DAYS>
```

Remediation:

Set the `PASS_MIN_DAYS` parameter to 7 in `/etc/login.defs`:

```
PASS_MIN_DAYS 7
```

Modify user parameters for all users with a password set to match:

```
# chage --mindays 7 <user>
```

Additional Information:

You can also check this setting in `/etc/shadow` directly. The 4th field should be 7 or more for all users with a password.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.12 Ensure password expiration warning days is 7 or more (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PASS_WARN_AGE` parameter in `/etc/login.defs` allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the `PASS_WARN_AGE` parameter be set to 7 or more days.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

Audit:

Run the following command and verify `PASS_WARN_AGE` conforms to site policy (No less than 7 days):

```
# grep PASS_WARN_AGE /etc/login.defs  
PASS_WARN_AGE 7
```

Verify all users with a password have their number of days of warning before password expires set to 7 or more:

Run the following command and Review list of users and `PASS_WARN_AGE` to verify that all users' `PASS_WARN_AGE` conforms to site policy (No less than 7 days):

```
# grep -E ^[^:]+:[^\\!*] /etc/shadow | cut -d: -f1,6  
<user>:<PASS_WARN_AGE>
```

Remediation:

Set the `PASS_WARN_AGE` parameter to 7 in `/etc/login.defs`:

```
PASS_WARN_AGE 7
```

Modify user parameters for all users with a password set to match:

```
# chage --warndays 7 <user>
```

Additional Information:

You can also check this setting in `/etc/shadow` directly. The 6th field should be 7 or more for all users with a password.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.13 Ensure inactive password lock is 30 days or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Audit:

Run the following command and verify INACTIVE conforms to site policy (no more than 30 days):

```
# useradd -D | grep INACTIVE  
INACTIVE=30
```

Verify all users with a password have Password inactive no more than 30 days after password expires:

Run the following command and Review list of users and INACTIVE to verify that all users' INACTIVE conforms to site policy (no more than 30 days):

```
# grep -E ^[^:]+:[^\\!*] /etc/shadow | cut -d: -f1,7  
<user>:<INACTIVE>
```

Remediation:

Run the following command to set the default password inactivity period to 30 days:

```
# useradd -D -f 30
```

Modify user parameters for all users with a password set to match:

```
# chage --inactive 30 <user>
```

Additional Information:

You can also check this setting in `/etc/shadow` directly. The 7th field should be 30 or less for all users with a password.

1 A value of -1 would disable this setting.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.14 Ensure all users last password change date is in the past (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

All users should have a password change date in the past.

Rationale:

If a user's recorded password change date is in the future then they could bypass any set password expiration.

Audit:

Run the following command and verify nothing is returned

```
# for usr in $(cut -d: -f1 /etc/shadow); do [[ $(chage --list $usr | grep '^Last password change' | cut -d: -f2) > $(date) ]] && echo "$usr :$(chage --list $usr | grep '^Last password change' | cut -d: -f2)"; done
```

Remediation:

Investigate any users with a password change date in the future and correct them. Locking the account, expiring the password, or resetting the password manually may be appropriate.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	●	●	●

5.5.1.15 Ensure the minimum time period between password changes for each user account is one day or greater (Automated)

Profile Applicability:

- STIG

Description:

Passwords must have a 24 hours/1 day minimum password lifetime restriction in "/etc/shadow".

Rationale:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Audit:

Check whether the minimum time period between password changes for each user account is one day or greater.

```
# awk -F: '$4 < 1 {print $1 " " $4}' /etc/shadow
```

If any results are returned that are not associated with a system account, this is a finding.

Remediation:

Configure non-compliant accounts to enforce a 24 hours/1 day minimum password lifetime:

```
# chage -m 1 [user]
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230364

Rule ID: SV-230364r627750_rule

STIG ID: RHEL-08-020180

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.16 Ensure the operating system enforces 24 hours/1 day as the minimum password lifetime for new user accounts (Automated)

Profile Applicability:

- STIG

Description:

Passwords for new users or password changes must have a 24 hours/1 day minimum password lifetime restriction in "/etc/login.defs".

Rationale:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Audit:

Verify the operating system enforces 24 hours/1 day as the minimum password lifetime for new user accounts.

Check for the value of "PASS_MIN_DAYS" in "/etc/login.defs" with the following command:

```
# grep -i pass_min_days /etc/login.defs  
PASS_MIN_DAYS 1
```

If the "PASS_MIN_DAYS" parameter value is not "1" or greater, or is commented out, this is a finding.

Remediation:

Configure the operating system to enforce 24 hours/1 day as the minimum password lifetime.

Add the following line in "/etc/login.defs" (or modify the line to have the required value):

```
PASS_MIN_DAYS 1
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230365

Rule ID: SV-230365r627750_rule

STIG ID: RHEL-08-020190

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

5.5.1.17 Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts (Automated)

Profile Applicability:

- STIG

Description:

User account passwords must have a 60-day maximum password lifetime restriction.

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system's passwords could be compromised.

Audit:

Verify that the operating system enforces a 60-day maximum password lifetime for new user accounts by running the following command:

```
# grep -i pass_max_days /etc/login.defs  
PASS_MAX_DAYS 60
```

If the "PASS_MAX_DAYS" parameter value is greater than "60", or commented out, this is a finding.

Remediation:

Configure the operating system to enforce a 60-day maximum password lifetime.

Add, or modify the following line in the "/etc/login.defs" file:

```
PASS_MAX_DAYS 60
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230366

Rule ID: SV-230366r646878_rule

STIG ID: RHEL-08-020200

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

5.5.1.18 Ensure the maximum time period for existing passwords is restricted to 60 days (Automated)

Profile Applicability:

- STIG

Description:

User account passwords must be configured so that existing passwords are restricted to a 60-day maximum lifetime.

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system's passwords could be compromised.

Audit:

Check whether the maximum time period for existing passwords is restricted to 60 days with the following commands:

```
# awk -F: '$5 > 60 {print $1 " " $5}' /etc/shadow  
# awk -F: '$5 <= 0 {print $1 " " $5}' /etc/shadow
```

If any results are returned that are not associated with a system account, this is a finding.

Remediation:

Configure non-compliant accounts to enforce a 60-day maximum password lifetime restriction.

```
# chage -M 60 [user]
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230367

Rule ID: SV-230367r627750_rule

STIG ID: RHEL-08-020210

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

5.5.1.19 Ensure the operating system enforces a minimum 15-character password length (Automated)

Profile Applicability:

- STIG

Description:

Passwords must have a minimum of 15 characters.

Rationale:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to increase exponentially the time and/or resources required to compromise the password.

RHEL 8 operating systems utilize "pwquality" as a mechanism to enforce password complexity. Configurations are set in the "etc/security/pwquality.conf" file.

The "minlen", sometimes noted as minimum length, acts as a "score" of complexity based on the credit components of the "pwquality" module. By setting the credit components to a negative value, not only will those components be required, they will not count towards the total "score" of "minlen". This will enable "minlen" to require a 15-character minimum. The DoD minimum password requirement is 15 characters.

Audit:

Verify the operating system enforces a minimum 15-character password length. The "minlen" option sets the minimum number of characters in a new password.

Check for the value of the "minlen" option in "/etc/security/pwquality.conf" with the following command:

```
# grep minlen /etc/security/pwquality.conf  
minlen = 15
```

If the command does not return a "minlen" value of 15 or greater, this is a finding.

Remediation:

Configure operating system to enforce a minimum 15-character password length.
Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
minlen = 15
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230369

Rule ID: SV-230369r627750_rule

STIG ID: RHEL-08-020230

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	●	●	●

5.5.1.20 Ensure the operating system enforces a minimum 15-character password length for new user accounts (Automated)

Profile Applicability:

- STIG

Description:

Passwords for new users must have a minimum of 15 characters.

Rationale:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to increase exponentially the time and/or resources required to compromise the password.

The DoD minimum password requirement is 15 characters.

Audit:

Verify that the operating system enforces a minimum 15-character password length for new user accounts by running the following command:

```
# grep -i pass_min_len /etc/login.defs  
PASS_MIN_LEN 15
```

If the "PASS_MIN_LEN" parameter value is less than "15", or commented out, this is a finding.

Remediation:

Configure operating system to enforce a minimum 15-character password length for new user accounts.

Add, or modify the following line in the "/etc/login.defs" file:

```
PASS_MIN_LEN 15
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230370

Rule ID: SV-230370r627750_rule

STIG ID: RHEL-08-020231

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.21 Ensure the value for "ocredit" in "/etc/security/pwquality.conf" is "-1" (Automated)

Profile Applicability:

- STIG

Description:

Passwords must contain at least one special character.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize "pwquality" as a mechanism to enforce password complexity. Note that to require special characters without degrading the "minlen" value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

Audit:

Verify the value for "ocredit" in "/etc/security/pwquality.conf" with the following command:

```
# grep ocredit /etc/security/pwquality.conf  
ocredit = -1
```

If the value of "ocredit" is a positive number or is commented out, this is a finding.

Remediation:

Configure the operating system to enforce password complexity by requiring that at least one special character be used by setting the "ocredit" option.

Add the following line to /etc/security/pwquality.conf (or modify the line to have the required value):

```
ocredit = -1
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230375

Rule ID: SV-230375r627750_rule

STIG ID: RHEL-08-020280

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.22 Ensure the operating system prevents the use of dictionary words for passwords (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent the use of dictionary words for passwords.

Rationale:

If the operating system allows the user to select passwords based on dictionary words, this increases the chances of password compromise by increasing the opportunity for successful guesses, and brute-force attacks.

Audit:

Verify the operating system prevents the use of dictionary words for passwords. Determine if the field "dictcheck" is set in the "/etc/security/pwquality.conf" or "/etc/pwquality.conf.d/*.conf" files with the following command:

```
# grep dictcheck /etc/security/pwquality.conf /etc/pwquality.conf.d/*.conf  
dictcheck=1
```

If the "dictcheck" parameter is not set to "1", or is commented out, this is a finding.

Remediation:

Configure the operating system to prevent the use of dictionary words for passwords. Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the /etc/pwquality.conf.d/ directory to contain the "dictcheck" parameter:

```
dictcheck=1
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230377

Rule ID: SV-230377r627750_rule

STIG ID: RHEL-08-020300

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.5.1.23 Ensure the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.

Rationale:

Configuring the operating system to implement organization-wide security implementation guides and security checklists verifies compliance with federal standards and establishes a common security baseline across the DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Audit:

Verify the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt with the following command:

```
# grep -i fail_delay /etc/login.defs  
FAIL_DELAY 4
```

If the value of "FAIL_DELAY" is not set to "4" or greater, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to enforce a delay of at least four seconds between logon prompts following a failed console logon attempt.

Modify the "/etc/login.defs" file to set the "FAIL_DELAY" parameter to "4" or greater:

```
FAIL_DELAY 4
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230378

Rule ID: SV-230378r627750_rule

STIG ID: RHEL-08-020310

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.5.2 Ensure system accounts are secured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

There are a number of accounts provided with most distributions that are used to manage applications and are not intended to provide an interactive shell.

Rationale:

It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, most distributions set the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to the `nologin` shell. This prevents the account from potentially being used to run any commands.

Audit:

Run the following commands and verify no results are returned:

```
awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" &&
$1!~/^+/ && $3<'$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)' &&
$7!="'"$(which nologin)"" && $7!="/bin/false") {print}' /etc/passwd

awk -F: '($1!="root" && $1~/^+/ && $3<'$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)'') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' |
awk '($2!="L" && $2!="LK") {print $1}'
```

Remediation:

Run the commands appropriate for your distribution:

Set the shell for any accounts returned by the audit to nologin:

```
# usermod -s $(which nologin) <user>
```

Lock any non root accounts returned by the audit:

```
# usermod -L <user>
```

The following command will set all system accounts to a non login shell:

```
awk -F: '$(1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $1!~/^+/ && $3<"$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)"' && $7!="'"$(which nologin)"'" && $7!="/bin/false") {print $1}' /etc/passwd | while read user do usermod -s $(which nologin) $user done
```

The following command will automatically lock not root system accounts:

```
awk -F: '$(1!="root" && $1!~/^+/ && $3<"$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' | awk '$2!="L" && $2!="LK") {print $1}' | while read user do usermod -L $user done
```

Additional Information:

The `root`, `sync`, `shutdown`, and `halt` users are exempted from requiring a non-login shell.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

5.5.3 Ensure default user shell timeout is 900 seconds or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`TMOUT` is an environmental setting that determines the timeout of a shell in seconds.

- `TMOUT=n` - Sets the shell timeout to *n* seconds. A setting of `TMOUT=0` disables timeout.
- `readonly TMOUT` - Sets the `TMOUT` environmental variable as readonly, preventing unwanted modification during run-time.
- `export TMOUT` - exports the `TMOUT` variable

System Wide Shell Configuration Files:

- `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `.bash_profile`, however this file is used to set an initial PATH or PS1 for all shell users of the system. **is only executed for interactive *login* shells, or shells executed with the --login parameter.**
- `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh`. It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
- `/etc/bashrc` - System wide version of `.bashrc`. In Fedora derived distributions, `etc/bashrc` also invokes `/etc/profile.d/*.sh` if *non-login* shell, but redirects output to `/dev/null` if *non-interactive*. **Is only executed for interactive shells or if BASH_ENV is set to /etc/bashrc.**

Rationale:

Setting a timeout value reduces the window of opportunity for unauthorized user access to another user's shell session that has been left unattended. It also ends the inactive session and releases the resources associated with that session.

Audit:

Run the following script to verify that TMOUT is configured to: include a timeout of no more than 900 seconds, to be readonly, to be exported, and is not being changed to a longer timeout.

```
#!/bin/bash

output1="" output2=""
[ -f /etc/bashrc ] && BRC="/etc/bashrc"
for f in "$BRC" /etc/profile /etc/profile.d/*.sh ; do
    grep -Pq '^s*([^\#]+\s+)?TMOUT=(900|[1-8][0-9][0-9]|[1-9][0-9]|1-9)\b' "$f" && grep -Pq '^s*([^\#]+;\s*)?readonly\s+TMOUT(\s+|\s*;|\s*$|=(900|[1-8][0-9][0-9]|[1-9][0-9]|1-9))\b' "$f" && grep -Pq '^s*([^\#]+;\s*)?export\s+TMOUT(\s+|\s*;|\s*$|=(900|[1-8][0-9][0-9]|[1-9][0-9]|1-9))\b' "$f" && output1="$f"
done
grep -Pq '^s*([^\#]+\s+)?TMOUT=(9[0-9][1-9]|9[1-9][0-9]|0+[1-9]\d{3,})\b' /etc/profile /etc/profile.d/*.sh "$BRC" && output2=$(grep -Ps '^s*([^\#]+\s+)?TMOUT=(9[0-9][1-9]|9[1-9][0-9]|0+[1-9]\d{3,})\b' /etc/profile /etc/profile.d/*.sh $BRC)
if [ -n "$output1" ] && [ -z "$output2" ]; then
    echo -e "\nPASSED\nTMOUT is configured in: \"$output1\"\n"
else
    [ -z "$output1" ] && echo -e "\nFAILED\nTMOUT is not configured\n"
    [ -n "$output2" ] && echo -e "\nFAILED\nTMOUT is incorrectly configured in: \"$output2\"\n"
fi
```

Remediation:

Review /etc/bashrc, /etc/profile, and all files ending in *.sh in the /etc/profile.d/ directory and remove or edit all TMOUT=_n_ entries to follow local site policy. TMOUT should not exceed 900 or be equal to 0.

Configure TMOUT in **one** of the following files:

- A file in the /etc/profile.d/ directory ending in .sh
- /etc/profile
- /etc/bashrc

TMOUT configuration examples:

As multiple lines:

```
TMOUT=900
readonly TMOUT
export TMOUT
```

As a single line:

```
readonly TMOUT=900 ; export TMOUT
```

Additional Information:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked. Other methods of setting a timeout exist for other shells not covered here. Ensure that the timeout conforms to your local policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	<u>16.11 Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

5.5.4 Ensure the interactive user account passwords are using a strong password hash (Automated)

Profile Applicability:

- STIG

Description:

The operating system must employ FIPS 140-2 approved cryptographic hashing algorithms for all stored passwords.

Rationale:

The system must use a strong hashing algorithm to store the password.

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Audit:

Confirm that the interactive user account passwords are using a strong password hash with the following command:

```
# cut -d: -f2 /etc/shadow  
  
$6$kcOnRq/5$NUEYPuyL.wghQwWssXRcLRFiiru7f5JPV6GaJhNC2aK5F3PZpE/BCCtwrxRc/AInK  
MNX3CdMw11m9STiq112f/
```

Password hashes "!" or "*" indicate inactive accounts not available for logon and are not evaluated. If any interactive user password hash does not begin with "\$6\$", this is a finding.

Remediation:

Lock all interactive user accounts not using SHA-512 hashing until the passwords can be regenerated with SHA-512.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230232

Rule ID: SV-230232r627750_rule

STIG ID: RHEL-08-010120

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

5.5.5 Ensure default group for the root account is GID 0 (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The usermod command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.

Rationale:

Using GID 0 for the `root` account helps prevent `root`-owned files from accidentally becoming accessible to non-privileged users.

Audit:

Run the following command and verify the result is 0 :

```
# grep "^\$root:" /etc/passwd | cut -f4 -d:  
0
```

Remediation:

Run the following command to set the `root` user default group to GID 0 :

```
# usermod -g 0 root
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.5.6 Ensure default user umask is 027 or more restrictive (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The user file-creation mode mask (`umask`) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (rwxrwxrwx), and for any newly created file it is 0666 (rw-rw-rw-). The `umask` modifies the default Linux permissions by restricting (masking) these permissions. The `umask` is not simply subtracted, but is processed bitwise. Bits set in the `umask` are cleared in the resulting file mode.

`umask` can be set with either `octal` or `Symbolic` values:

- `Octal` (Numeric) Value - Represented by either three or four digits. ie `umask 0027` or `umask 027`. If a four digit `umask` is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- `Symbolic` Value - Represented by a comma separated list for User `u`, group `g`, and world/other `o`. The permissions listed are not masked by `umask`. ie a `umask` set by `umask u=rwx, g=rx, o=` is the `Symbolic` equivalent of the `Octal` `umask 027`. This `umask` would set a newly created directory with file mode `drwxr-x---` and a newly created file with file mode `rw-r----`.

The default `umask` can be set to use the `pam_umask` module or in a System Wide Shell Configuration File. The user creating the directories or files has the discretion of changing the permissions via the `chmod` command, or choosing a different default `umask` by adding the `umask` command into a User Shell Configuration File, (`.bash_profile` or `.bashrc`), in their home directory.

Setting the default `umask`:

- `pam_umask` module:
 - will set the `umask` according to the system default in `/etc/login.defs` and user settings, solving the problem of different `umask` settings with different shells, display managers, remote sessions etc.
 - `umask=<mask>` value in the `/etc/login.defs` file is interpreted as Octal
 - Setting `USERGROUPS_ENAB` to yes in `/etc/login.defs` (default):
 - will enable setting of the `umask` group bits to be the same as owner bits. (examples: 022 -> 002, 077 -> 007) for non-root users, if the `uid` is the same as `gid`, and `username` is the same as the `<primary group name>`
 - `userdel` will remove the user's group if it contains no more members, and `useradd` will create by default a group with the name of the user
- System Wide Shell Configuration File:

- `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `.bash_profile`, however this file is used to set an initial PATH or PS1 for all shell users of the system. **is only executed for interactive *login shells*, or shells executed with the --login parameter.**
- `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh`. It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
- `/etc/bashrc` - System wide version of `.bashrc`. In Fedora derived distributions, `etc/bashrc` also invokes `/etc/profile.d/*.sh` if *non-login* shell, but redirects output to `/dev/null` if *non-interactive*. **Is only executed for interactive shells or if BASH_ENV is set to /etc/bashrc.**

User Shell Configuration Files:

- `~/.bash_profile` - Is executed to configure your shell before the initial command prompt. **Is only read by login shells.**
- `~/.bashrc` - Is executed for interactive shells. **only read by a shell that's both interactive and non-login**

Rationale:

Setting a very secure default value for `umask` ensures that users make a conscious choice about their file permissions. A default `umask` setting of `077` causes files and directories created by users to not be readable by any other user on the system. A `umask` of `027` would make files and directories readable by users in the same Unix group, while a `umask` of `022` would make files readable by every user on the system.

Audit:

Run the following to verify:

- A default user umask is set to enforce a newly created directories' permissions to be 750 (drwxr-x---), and a newly created file's permissions be 640 (rw-r-----), or more restrictive
- No less restrictive System Wide umask is set

Run the following script to verify that a default user umask is set enforcing a newly created directories's permissions to be 750 (drwxr-x---), and a newly created file's permissions be 640 (rw-r-----), or more restrictive:

```
#!/bin/bash

passing=""
grep -Eq '^\s*UMASK\s+(0[0-7][2-7]7|[0-7][2-7]7)\b' /etc/login.defs && grep -Eqi '^s*USERGROUPS_ENAB\s*"no"\b' /etc/login.defs && grep -Eq '^s*session\s+(optional|requisite|required)\s+pam_umask\.so\b' /etc/pam.d/common-session && passing=true
grep -REiq '^\s*UMASK\s+\s*(0[0-7][2-7]7|[0-7][2-7]7|u=(r?|w?|x?)(r?|w?|x?)(r?|w?|x?),g=(r?x?|x?r?),o=)\b' /etc/profile* /etc/bashrc* && passing=true
[ "$passing" = true ] && echo "Default user umask is set"
```

Verify output is: "Default user umask is set"

Run the following to verify that no less restrictive system wide umask is set:

```
# grep -RPi '^(|^[^#]* )\s*umask\s+([0-7][0-7][01][0-7]\b|[0-7][0-7][0-6]\b|[0-7][01][0-7]\b|[0-7][0-7][0-6]\b|(u=[rwx]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+\b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(,o=[rwx]{0,3})?\b)' /etc/login.defs /etc/profile* /etc/bashrc*
```

No file should be returned

Remediation:

Review `/etc/bashrc`, `/etc/profile`, and all files ending in `*.sh` in the `/etc/profile.d/` directory and remove or edit all `umask` entries to follow local site policy. Any remaining entries should be: `umask 027`, `umask u=rwx, g=rx, o=` or more restrictive.

Configure `umask` in **one** of the following files:

- A file in the `/etc/profile.d/` directory ending in `.sh`
- `/etc/profile`
- `/etc/bashrc`

```
# vi /etc/profile.d/set_umask.sh  
umask 027
```

Run the following command and remove or modify the `umask` of any returned files:

```
# grep -RPi '^(^|[^#]* )\s*umask\s+(([0-7][0-7][01][0-7]\b|[0-7][0-7][0-7][0-6]\b|[0-7][01][0-7]\b|[0-7][0-7]\b|[0-6]\b|(u=[rwx]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+\b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(,o=[rwx]{0,3})?\b)' /etc/login.defs /etc/profile* /etc/bashrc*
```

Follow one of the following methods to set the default user umask:

Edit `/etc/login.defs` and edit the `UMASK` and `USERGROUPS_ENAB` lines as follows:

```
UMASK 027  
USERGROUPS_ENAB no
```

Edit the files `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` and add or edit the following:

```
session optional pam_umask.so
```

Or

Configure umask in one of the following files:

- A file in the `/etc/profile.d/` directory ending in `.sh`
- `/etc/profile`
- `/etc/bashrc`

Example: /etc/profile.d/set_umask.sh

```
umask 027
```

Note: this method only applies to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked.

Default Value:

UMASK 022

Additional Information:

- Other methods of setting a default user umask exist
- If other methods are in use in your environment they should be audited
- The default user umask can be overridden with a user specific umask
- The user creating the directories or files has the discretion of changing the permissions:
 - Using the chmod command
 - Setting a different default umask by adding the umask command into a User Shell Configuration File, (.bashrc), in their home directory
 - Manually changing the umask for the duration of a login session by running the umask command

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	13 Data Protection Data Protection			

5.5.7 Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity (Automated)

Profile Applicability:

- STIG

Description:

Account identifiers (individuals, groups, roles, and devices) must be disabled after 35 days of inactivity.

Rationale:

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

The operating system needs to track periods of inactivity and disable application identifiers after 35 days of inactivity.

Audit:

Verify the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity with the following command:

Check the account inactivity value by performing the following command:

```
# grep -i inactive /etc/default/useradd  
INACTIVE=35
```

If "INACTIVE" is set to "-1", a value greater than "35", or is commented out, this is a finding.

Remediation:

Configure the operating system to disable account identifiers after 35 days of inactivity after the password expiration.

Run the following command to change the configuration for useradd:

```
# useradd -D -f 35
```

DoD recommendation is 35 days, but a lower value is acceptable. The value "-1" will disable this feature, and "0" will disable the account immediately after the password expires.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230373

Rule ID: SV-230373r627750_rule

STIG ID: RHEL-08-020260

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.9 Disable Dormant Accounts Automatically disable dormant accounts after a set period of inactivity.	●	●	●

5.5.8 Ensure emergency accounts have been provisioned with an expiration date of 72 hours (Manual)

Profile Applicability:

- STIG

Description:

Emergency accounts must be automatically removed or disabled after the crisis is resolved or within 72 hours.

Rationale:

Emergency accounts are privileged accounts established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are automatically disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Emergency accounts are different from infrequently used accounts (i.e., local logon accounts used by the organization's system administrators when network or normal logon/access is not available). Infrequently used accounts are not subject to automatic termination dates. Emergency accounts are accounts created in response to crisis situations, usually for use by maintenance personnel. The automatic expiration or disabling time period may be extended as needed until the crisis is resolved; however, it must not be extended indefinitely. A permanent account should be established for privileged users who need long-term maintenance accounts.

To address access requirements, many RHEL operating systems can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Audit:

Verify emergency accounts have been provisioned with an expiration date of 72 hours. For every existing emergency account, run the following command to obtain its account expiration information.

```
# chage -l system_account_name
```

Verify each of these accounts has an expiration date set within 72 hours. If any emergency accounts have no expiration date set or do not expire within 72 hours, this is a finding.

Remediation:

If an emergency account must be created, configure the system to terminate the account after 72 hours with the following command to set an expiration date for the account.

Substitute "system_account_name" with the account to be created.

```
# chage -E `date -d "+3 days" +%Y-%m-%d` system_account_name
```

The automatic expiration or disabling time period may be extended as needed until the crisis is resolved.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230374

Rule ID: SV-230374r627750_rule

STIG ID: RHEL-08-020270

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.5.9 Ensure the default umask for all local interactive users is "077" (Manual)

Profile Applicability:

- STIG

Description:

The operating system must set the umask value to 077 for all local interactive user accounts.

Rationale:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 600 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be "0". This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Audit:

Verify that the default umask for all local interactive users is "077".

Identify the locations of all local interactive user home directories by looking at the "/etc/passwd" file.

Check all local interactive user initialization files for interactive users with the following command:

Note: The example is for a system that is configured to create users home directories in the "/home" directory.

```
# grep -i umask /home/*/.*
```

If any local interactive user initialization files are found to have a umask statement that has a value less restrictive than "077", this is a finding.

Remediation:

Remove the umask statement from all local interactive user's initialization files.

If the account is for an application, the requirement for a umask less restrictive than "077" can be documented with the Information System Security Officer, but the user agreement for access to the account must specify that the local interactive user must log on to their account first and then switch the user to the application account with the correct option to gain the account's environment variables.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230384

Rule ID: SV-230384r627750_rule

STIG ID: RHEL-08-020352

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	13 Data Protection Data Protection			

5.5.10 Ensure the umask default for installed shells is "077" (Automated)

Profile Applicability:

- STIG

Description:

The operating system must define default permissions for logon and non-logon shells.

Rationale:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 600 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be "0". This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Audit:

Verify that the umask default for installed shells is "077".

Check for the value of the "UMASK" parameter in the "/etc/bashrc" and "/etc/csh.cshrc" files with the following command:

Note: If the value of the "UMASK" parameter is set to "000" in either the "/etc/bashrc" or the "/etc/csh.cshrc" files, the Severity is raised to a CAT I.

```
# grep -i umask /etc/bashrc /etc/csh.cshrc  
  
/etc/bashrc: umask 077  
/etc/bashrc: umask 077  
/etc/csh.cshrc: umask 077  
/etc/csh.cshrc: umask 077
```

If the value for the "UMASK" parameter is not "077", or the "UMASK" parameter is missing or is commented out, this is a finding.

Remediation:

Configure the operating system to define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Add or edit the lines for the "UMASK" parameter in the "/etc/bashrc" and "/etc/csh.cshrc" files to "077":

```
UMASK 077
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230385

Rule ID: SV-230385r627750_rule

STIG ID: RHEL-08-020353

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	13 Data Protection Data Protection			

5.5.11 Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files (Automated)

Profile Applicability:

- STIG

Description:

The operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Rationale:

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Audit:

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Check Text: Verify the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Check for the value of the "UMASK" parameter in "/etc/login.defs" file with the following command:

Note: If the value of the "UMASK" parameter is set to "000" in "/etc/login.defs" file, the Severity is raised to a CAT I.

```
# grep -i umask /etc/login.defs  
UMASK 077
```

If the value for the "UMASK" parameter is not "077", or the "UMASK" parameter is missing or is commented out, this is a finding.

Remediation:

Configure the operating system to define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Add or edit the line for the "UMASK" parameter in "/etc/login.defs" file to "077":

```
UMASK 077
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230383

Rule ID: SV-230383r627750_rule

STIG ID: RHEL-08-020351

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	13 Data Protection Data Protection			

5.6 Ensure root login is restricted to system console (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The file `/etc/securetty` contains a list of valid terminals that may be logged in directly as root.

Rationale:

Since the system console has special properties to handle emergency situations, it is important to ensure that the console is in a physically secure location and that unauthorized consoles have not been defined.

Audit:

```
# cat /etc/securetty
```

Remediation:

Remove entries for any consoles that are not in a physically secure location.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.7 Ensure PKI-based authentication has valid certificates (Manual)

Profile Applicability:

- STIG

Description:

The operating system must validate certificates for PKI-based authentication by constructing a certification path (which includes status information) to an accepted trust anchor.

Rationale:

Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC. When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a Certification Authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

This requirement verifies that a certification path to an accepted trust anchor is used for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses. Validation of the certificate status information is out of scope for this requirement.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000384-GPOS-00167

Audit:

Verify PKI-based authentication has valid certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

Check that the system has a valid DoD root CA installed with the following command:

```
# openssl x509 -text -in /etc/sssd/pki/sssd_auth_ca_db.pem  
  
Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number: 1 (0x1)  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: C = US, O = U.S. Government, OU = DoD, OU = PKI, CN = DoD Root CA 3  
Validity  
Not Before: Mar 20 18:46:41 2012 GMT  
Not After : Dec 30 18:46:41 2029 GMT  
Subject: C = US, O = U.S. Government, OU = DoD, OU = PKI, CN = DoD Root CA 3  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption
```

If the root ca file is not a DoD-issued certificate with a valid date and installed in the "/etc/sssd/pki/sssd_auth_ca_db.pem" location, this is a finding.

Remediation:

Configure PKI-based authentication to validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

Obtain a valid copy of the DoD root CA file from the PKI CA certificate bundle from cyber.mil and copy the "DoD_PKE_CA_chain.pem" into the following file:

```
/etc/sssd/pki/sssd_auth_ca_db.pem
```

Additional Information:

```
Red Hat Enterprise Linux 8 Security Technical Implementation Guide
```

```
Version 1, Release: 3 Benchmark Date: 23 Jul 2021
```

```
Vul ID: V-230229
```

```
Rule ID: SV-230229r627750_rule
```

```
STIG ID: RHEL-08-010090
```

```
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.8 Ensure access to the su command is restricted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `su` command allows a user to run a command or shell as another user. The program has been superseded by `sudo`, which allows for more granular control over privileged access. Normally, the `su` command can be executed by any user. By uncommenting the `pam_wheel.so` statement in `/etc/pam.d/su`, the `su` command will only allow users in the `wheel` group to execute `su`.

Rationale:

Restricting the use of `su`, and using `sudo` in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The `sudo` utility also provides a better logging and audit mechanism, as it can log each command executed via `sudo`, whereas `su` can only record that a user executed the `su` program.

Audit:

Run the following command and verify output includes matching line:

```
# grep pam_wheel.so /etc/pam.d/su
auth required pam_wheel.so use_uid
```

Run the following command and verify users in `wheel` group match site policy. If no users are listed, only root will have access to `su`.

```
# grep wheel /etc/group
wheel:x:10:root,<user list>
```

Remediation:

Add the following line to the `/etc/pam.d/su` file:

```
auth required pam_wheel.so use_uid
```

Create a comma separated list of users in the `wheel` statement in the `/etc/group` file:

```
wheel:x:<GID>:root,<user list>
```

Example:

```
wheel:x:10:root,user1,user2,user3
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.9 Ensure the operating system prevents system daemons from using Kerberos for authentication (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent system daemons from using Kerberos for authentication.

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

The key derivation function (KDF) in Kerberos is not FIPS compatible. Ensuring the system does not have any keytab files present prevents system daemons from using Kerberos for authentication. A keytab is a file containing pairs of Kerberos principals and encrypted keys.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

Audit:

Verify that the operating system prevents system daemons from using Kerberos for authentication.

If the system is a server utilizing krb5-server-1.17-18.el8.x86_64 or newer, this requirement is not applicable.

If the system is a workstation utilizing krb5-workstation-1.17-18.el8.x86_64 or newer, this requirement is not applicable.

Check if there are available keytabs with the following command:

```
# ls -al /etc/*.keytab
```

If this command produces any file(s), this is a finding.

Remediation:

Configure the operating system to prevent system daemons from using Kerberos for authentication.

Remove any files with the .keytab extension from the operating system.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide
Version 1, Release: 3 Benchmark Date: 23 Jul 2021
Vul ID: V-230238
Rule ID: SV-230238r646862_rule
STIG ID: RHEL-08-010161
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.10 Ensure the krb5-workstation package has not been installed on the system (Automated)

Profile Applicability:

- STIG

Description:

The krb5-workstation package must not be installed on the operating system.

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

Currently, Kerberos does not utilize FIPS 140-2 cryptography.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

Audit:

Verify the krb5-workstation package has not been installed on the system with the following commands:

If the system is a server or is utilizing krb5-workstation-1.17-18.el8.x86_64 or newer, this is Not Applicable.

```
# dnf list installed krb5-workstation  
krb5-workstation.x86_64 1.17-9.el8 repository
```

If the krb5-workstation package is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the krb5-workstation package with the ISSO as an operational requirement or remove it from the system with the following command:

```
# dnf remove krb5-workstation
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230239

Rule ID: SV-230239r646864_rule

STIG ID: RHEL-08-010162

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

5.11 Ensure SSSD prohibits the use of cached authentications after one day (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prohibit the use of cached authentications after one day.

Rationale:

If cached authentication information is out-of-date, the validity of the authentication information may be questionable.

The operating system includes multiple options for configuring authentication, but this requirement will focus on the System Security Services Daemon (SSSD). By default sssd does not cache credentials.

Audit:

Verify that the SSSD prohibits the use of cached authentications after one day.

Note: If smart card authentication is not being used on the system this item is Not Applicable.

Check that SSSD allows cached authentications with the following command:

```
# grep cache_credentials /etc/sssd/sssd.conf  
cache_credentials = true
```

If "cache_credentials" is set to "false" or missing from the configuration file, this is not a finding and no further checks are required.

If "cache_credentials" is set to "true", check that SSSD prohibits the use of cached authentications after one day with the following command:

```
# grep offline_credentials_expiration /etc/sssd/sssd.conf  
offline_credentials_expiration = 1
```

If "offline_credentials_expiration" is not set to a value of "1", this is a finding.

Remediation:

Configure the SSSD to prohibit the use of cached authentications after one day.
Add or change the following line in "/etc/sssd/sssd.conf" just below the line "[pam]".

```
offline_credentials_expiration = 1
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230376

Rule ID: SV-230376r627750_rule

STIG ID: RHEL-08-020290

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.12 Ensure "fapolicyd" is installed (Automated)

Profile Applicability:

- STIG

Description:

The "fapolicy" module must be installed.

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. Utilizing a whitelist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities. Verification of whitelisted software occurs prior to execution or at system startup.

User home directories/folders may contain information of a sensitive nature. Non-privileged users should coordinate any sharing of information with an SA through shared resources.

RHEL 8 operating system's ship with many optional packages. One such package is a file access policy daemon called "fapolicyd". "fapolicyd" is a userspace daemon that determines access rights to files based on attributes of the process and file. It can be used to either blacklist or whitelist processes or file access.

Proceed with caution with enforcing the use of this daemon. Improper configuration may render the system non-functional. The "fapolicyd" API is not namespace aware and can cause issues when launching or running containers.

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155, SRG-OS-000480-GPOS-00232

Audit:

Verify that "fapolicyd" is installed.

Check that "fapolicyd" is installed with the following command:

```
# dnf list installed fapolicyd  
Installed Packages  
fapolicyd.x86_64
```

If fapolicyd is not installed, this is a finding.

Remediation:

Install "fapolicyd" with the following command:

```
# dnf install fapolicyd.x86_64
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230523

Rule ID: SV-230523r744023_rule

STIG ID: RHEL-08-040135

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.13 Ensure USBDaemon has a policy configured (Manual)

Profile Applicability:

- STIG

Description:

The operating system must block unauthorized peripherals before establishing a connection.

Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include, but are not limited to, such devices as flash drives, external storage, and printers.

A new feature that RHEL 8 operating system's provide is the USBDaemon software framework. The USBDaemon-daemon is the main component of the USBDaemon software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices. The policy is defined by a set of rules using a rule language described in the usbdamond-rules.conf file. The policy and the authorization state of USB devices can be modified during runtime using the USBDaemon tool.

The System Administrator (SA) must work with the site Information System Security Officer (ISSO) to determine a list of authorized peripherals and establish rules within the USBDaemon software framework to allow only authorized devices.

Audit:

Verify the USBDaemon has a policy configured with the following command:

```
# usbdamond list-rules
```

If the command does not return results or an error is returned, ask the SA to indicate how unauthorized peripherals are being blocked.

If there is no evidence that unauthorized peripherals are being blocked before establishing a connection, this is a finding.

Remediation:

Configure the operating system to enable the blocking of unauthorized peripherals with the following command:

This command must be run from a root shell and will create an allow list for any USB devices currently connect to the system.

```
# usbguard generate-policy > /etc/usbguard/rules.conf
```

Note: Enabling and starting USBguard without properly configuring it for an individual system will immediately prevent any access over a USB device such as a keyboard or mouse

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230524

Rule ID: SV-230524r744026_rule

STIG ID: RHEL-08-040140

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	13.7 Manage USB Devices If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.	●	●	●

5.14 Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement DoD-approved encryption in the OpenSSL package.

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 8 operating systems incorporate system-wide crypto policies by default. The employed algorithms can be viewed in the /etc/crypto-policies/back-ends/openssl.config file.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000125-GPOS-00065

Audit:

Verify the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms:

Verify that system-wide crypto policies are in effect:

```
# grep -i opensslcnf.config /etc/pki/tls/openssl.cnf  
.include /etc/crypto-policies/back-ends/opensslcnf.config
```

If the "opensslcnf.config" is not defined in the "/etc/pki/tls/openssl.cnf" file, this is a finding.

Verify which system-wide crypto policy is in use:

```
# update-crypto-policies --show  
FIPS
```

If the system-wide crypto policy is set to anything other than "FIPS", this is a finding.

Remediation:

Configure the OpenSSL library to use only ciphers employing FIPS 140-2-approved algorithms with the following command:

```
# fips-mode-setup --enable
```

A reboot is required for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230254

Rule ID: SV-230254r627750_rule

STIG ID: RHEL-08-010293

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

5.15 Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement DoD-approved TLS encryption in the OpenSSL package.

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 8 operating systems incorporate system-wide crypto policies by default. The employed algorithms can be viewed in the /etc/crypto-policies/back-ends/openssl.config file.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000125-GPOS-00065

Audit:

Verify the OpenSSL library is configured to use only DoD-approved TLS encryption:

```
# grep -i MinProtocol /etc/crypto-policies/back-ends/opensslcnf.config  
MinProtocol = TLSv1.2
```

If the "MinProtocol" is set to anything older than "TLSv1.2", this is a finding.

Remediation:

Configure the OpenSSL library to use only DoD-approved TLS encryption by editing the following line in the "/etc/crypto-policies/back-ends/opensslcnf.config" file:

```
MinProtocol = TLSv1.2
```

A reboot is required for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230255

Rule ID: SV-230255r627750_rule

STIG ID: RHEL-08-010294

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.			

5.16 Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement DoD-approved TLS encryption in the GnuTLS package.

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Transport Layer Security (TLS) encryption is a required security setting as a number of known vulnerabilities have been reported against Secure Sockets Layer (SSL) and earlier versions of TLS. Encryption of private information is essential to ensuring data confidentiality. If private information is not encrypted, it can be intercepted and easily read by an unauthorized party. SQL Server must use a minimum of FIPS 140-2-approved TLS version 1.2, and all non-FIPS-approved SSL and TLS versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

The GnuTLS library offers an API to access secure communications protocols. SSLv2 is not available in the GnuTLS library. The operating system's system-wide crypto policy defines employed algorithms in the /etc/crypto-policies/back-ends/gnutls.config file.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000423-GPOS-00187

Audit:

Verify the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions:

```
# grep -io +vers.* /etc/crypto-policies/back-ends/gnutls.config  
+VERS-ALL:-VERS-DTLS0.9:-VERS-SSL3.0:-VERS-TLS1.0:-VERS-TLS1.1:-VERS-  
DTLS1.0:+COMP-NULL:%PROFILE_MEDIUM
```

If the "gnutls.config" does not list "-VERS-DTLS0.9:-VERS-SSL3.0:-VERS-TLS1.0:-VERS-TLS1.1:VERS-DTLS1.0" to disable unapproved SSL/TLS versions, this is a finding.

Remediation:

Configure the operating system's GnuTLS library to use only DoD-approved encryption by adding the following line to "/etc/crypto-policies/back-ends/gnutls.config":

```
+VERS-ALL:-VERS-DTLS0.9:-VERS-SSL3.0:-VERS-TLS1.0:-VERS-TLS1.1:-VERS-DTLS1.0
```

A reboot is required for the changes to take effect.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230256

Rule ID: SV-230256r627750_rule

STIG ID: RHEL-08-010295

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.			

5.17 Ensure "fapolicyd" is enabled and running (Automated)

Profile Applicability:

- STIG

Description:

The "fapolic4y" module must be enabled.

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. Utilizing a whitelist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities. Verification of whitelisted software occurs prior to execution or at system startup.

User home directories/folders may contain information of a sensitive nature. Non-privileged users should coordinate any sharing of information with an SA through shared resources.

RHEL 8 operating systems ship with many optional packages. One such package is a file access policy daemon called "fapolicyd". "fapolicyd" is a userspace daemon that determines access rights to files based on attributes of the process and file. It can be used to either blacklist or whitelist processes or file access.

Proceed with caution with enforcing the use of this daemon. Improper configuration may render the system non-functional. The "fapolicyd" API is not namespace aware and can cause issues when launching or running containers.

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155, SRG-OS-000480-GPOS-00232

Audit:

Verify "fapolicyd" is enabled and running with the following command:

```
# systemctl status fapolicyd.service
fapolicyd.service - File Access Policy Daemon
Loaded: loaded (/usr/lib/systemd/system/fapolicyd.service; enabled; vendor
preset: disabled)
Active: active (running)
```

If fapolicyd is not enabled and running, this is a finding.

Remediation:

Enable "fapolicyd" using the following command:

```
# systemctl enable --now fapolicyd
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244545

Rule ID: SV-244545r743884_rule

STIG ID: RHEL-08-040136

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

5.18 Ensure "fapolicyd" employs a deny-all, permit-by-exception policy (Automated)

Profile Applicability:

- STIG

Description:

The "fapolicy" module must be configured to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. Utilizing a whitelist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities. Verification of whitelisted software occurs prior to execution or at system startup.

User home directories/folders may contain information of a sensitive nature. Non-privileged users should coordinate any sharing of information with an SA through shared resources.

RHEL 8 operating systems ship with many optional packages. One such package is a file access policy daemon called "fapolicyd". "fapolicyd" is a userspace daemon that determines access rights to files based on attributes of the process and file. It can be used to either blacklist or whitelist processes or file access.

Proceed with caution with enforcing the use of this daemon. Improper configuration may render the system non-functional. The "fapolicyd" API is not namespace aware and can cause issues when launching or running containers.

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155, SRG-OS-000480-GPOS-00232

Audit:

Verify the operating system's "fapolicyd" employs a deny-all, permit-by-exception policy.

Check that "fapolicyd" is in enforcement mode with the following command:

```
# grep permissive /etc/fapolicyd/fapolicyd.conf  
permissive = 0
```

Check that "fapolicyd" employs a deny-all policy on system mounts with the following commands:

```
# tail /etc/fapolicyd/fapolicyd.rules  
  
allow exe=/usr/bin/python3.7 : ftype=text/x-python  
deny_audit perm=any pattern=ld_so : all  
deny perm=any all : all  
  
# cat /etc/fapolicyd/fapolicyd.mounts  
  
/dev/shm  
/run  
/sys/fs/cgroup  
/  
/home  
/boot  
/run/user/42  
/run/user/1000
```

If "fapolicyd" is not running in enforcement mode on all system mounts with a deny-all, permit-by-exception policy, this is a finding.

Remediation:

Configure the operating system to employ a deny-all, permit-by-exception application whitelisting policy with "fapolicyd" using the following command:

Note: Running this command requires a root shell

```
# mount | egrep '^tmpfs| ext4| ext3| xfs' | awk '{ printf "%s\n", $3 }' >> /etc/fapolicyd/fapolicyd.mounts
```

With the "fapolicyd" installed and enabled, configure the daemon to function in permissive mode until the whitelist is built correctly to avoid system lockout. Do this by editing the "/etc/fapolicyd/fapolicyd.conf" file with the following line:

```
permissive = 1
```

Build the whitelist in the "/etc/fapolicyd/fapolicyd.rules" file ensuring the last rule is "deny perm=any all : all".

Once it is determined the whitelist is built correctly, set fapolicyd to enforcing mode by editing the "permissive" line in the "/etc/fapolicyd/fapolicyd.conf" file.

```
permissive = 0
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244546

Rule ID: SV-244546r743887_rule

STIG ID: RHEL-08-040137

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

5.19 Ensure USBDaemon is installed on the operating system (Automated)

Profile Applicability:

- STIG

Description:

The operating system must have USBDaemon installed.

Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include, but are not limited to, such devices as flash drives, external storage, and printers.

A new feature that RHEL 8 operating systems provide is the USBDaemon software framework. The USBDaemon-daemon is the main component of the USBDaemon software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices. The policy is defined by a set of rules using a rule language described in the "usbdammon-rules.conf" file. The policy and the authorization state of USB devices can be modified during runtime using the USBDaemon tool.

The System Administrator (SA) must work with the site Information System Security Officer (ISSO) to determine a list of authorized peripherals and establish rules within the USBDaemon software framework to allow only authorized devices.

Audit:

Verify USBDaemon is installed on the operating system with the following command:

```
# dnf list installed usbdammon  
Installed Packages  
usbdammon.x86_64 0.7.8-7.el8 @ol8_appstream
```

If the USBDaemon package is not installed, ask the SA to indicate how unauthorized peripherals are being blocked.

If there is no evidence that unauthorized peripherals are being blocked before establishing a connection, this is a finding.

Remediation:

Install the USBDaemon package with the following command:

```
# dnf install usbdammon.x86_64
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244547

Rule ID: SV-244547r743890_rule

STIG ID: RHEL-08-040139

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	13.7 Manage USB Devices If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.			

5.20 Ensure the operating system has enabled the use of the USBDaemon (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enable USBDaemon.

Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include, but are not limited to, such devices as flash drives, external storage, and printers.

A new feature that RHEL 8 operating systems provide is the USBDaemon software framework. The USBDaemon-daemon is the main component of the USBDaemon software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices. The policy is defined by a set of rules using a rule language described in the "usbdamond-rules.conf" file. The policy and the authorization state of USB devices can be modified during runtime using the USBDaemon tool.

The System Administrator (SA) must work with the site Information System Security Officer (ISSO) to determine a list of authorized peripherals and establish rules within the USBDaemon software framework to allow only authorized devices.

Audit:

Verify the operating system has enabled the use of the USBDaemon with the following command:

```
# systemctl status usbdamond.service

usbdamond.service - USBDaemon daemon
Loaded: loaded (/usr/lib/systemd/system/usbdamond.service; enabled; vendor
preset: disabled)
Active: active (running)
```

If the usbdamond.service is not enabled and active, ask the SA to indicate how unauthorized peripherals are being blocked.

If there is no evidence that unauthorized peripherals are being blocked before establishing a connection, this is a finding.

Remediation:

Configure the operating system to enable the blocking of unauthorized peripherals with the following commands:

```
# systemctl enable usbguard.service  
# systemctl start usbguard.service
```

Note: Enabling and starting USBGuard without properly configuring it for an individual system will immediately prevent any access over a USB device such as a keyboard or mouse.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244548

Rule ID: SV-244548r743893_rule

STIG ID: RHEL-08-040141

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	13.7 Manage USB Devices If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.		●	●

6 System Maintenance

Recommendations in this section are intended as maintenance and are intended to be checked on a frequent basis to ensure system stability. Many recommendations do not have quick remediations and require investigation into the cause and best fix available and may indicate an attempted breach of system security.

6.1 System File Permissions

This section provides guidance on securing aspects of system files and directories.

6.1.1 Audit system file permissions (Manual)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The RPM package manager has a number of useful options. One of these, the `-v` for RPM option, can be used to verify that system packages are correctly installed. The `-v` option can be used to verify a particular package or to verify all system packages. If no output is returned, the package is installed correctly. The following table describes the meaning of output from the verify option:

Code	Meaning
S	File size differs.
M	File mode differs (includes permissions and file type).
5	The MD5 checksum differs.
D	The major and minor version numbers differ on a device file.
L	A mismatch occurs in a link.
U	The file ownership differs.
G	The file group owner differs.
T	The file time (mtime) differs.

The `rpm -qf` command can be used to determine which package a particular file belongs to. For example the following commands determines which package the `/bin/bash` file belongs to:

```
# rpm -qf /bin/bash
bash-4.1.2-29.el6.x86_64
# dpkg -S /bin/bash
bash: /bin/bash
```

To verify the settings for the package that controls the `/bin/bash` file, run the following:

```
# rpm -V bash-4.1.2-29.el6.x86_64  
.M..... /bin/bash  
# dpkg --verify bash  
??5?????? c /etc/bash.bashrc
```

Note that you can feed the output of the `rpm -qf` command to the `rpm -V` command:

```
# rpm -V `rpm -qf /etc/passwd`  
.M..... c /etc/passwd  
S.5....T c /etc/printcap
```

Rationale:

It is important to confirm that packaged system files and directories are maintained with the permissions they were intended to have from the OS vendor.

Audit:

Run the following command to review all installed packages. Note that this may be very time consuming and may be best scheduled via the `cron` utility. It is recommended that the output of this command be redirected to a file that can be reviewed later.

```
# rpm -Va --nomtime --nosize --nomd5 --nolinkto > <filename>
```

Remediation:

Correct any discrepancies found and rerun the audit until output is clean or risk is mitigated or accepted.

References:

1. http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/index.html

Additional Information:

Since packages and important files may change with new updates and releases, it is recommended to verify everything, not just a finite list of files. This can be a time consuming task and results may depend on site policy therefore it is not a scorable benchmark item, but is provided for those interested in additional security measures. Some of the recommendations of this benchmark alter the state of files audited by this recommendation. The audit command will alert for all changes to a file permissions even if the new state is more secure than the default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.2 Ensure permissions on /etc/passwd are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/passwd` file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

Rationale:

It is critical to ensure that the `/etc/passwd` file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` or more restrictive:

```
# stat /etc/passwd
Access: (0644/-rw-r--r--)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following command to set permissions on `/etc/passwd`:

```
# chown root:root /etc/passwd
# chmod 644 /etc/passwd
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.1.3 Ensure permissions on /etc/passwd- are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The /etc/passwd- file contains backup user account information.

Rationale:

It is critical to ensure that the /etc/passwd- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command and verify Uid and Gid are both 0/root and Access is 644 or more restrictive:

```
# stat /etc/passwd-
Access: (0644/-rw-r--r--) Uid: ( 0/    root)  Gid: ( 0/    root)
```

Remediation:

Run the following commands to set owner, group, and permissions on /etc/passwd-:

```
# chown root:root /etc/passwd-
# chmod chmod u-x,go-wx /etc/passwd-
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.1.4 Ensure permissions on /etc/shadow are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/shadow` file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert the user accounts.

Audit:

Run the following command and verify Uid and Gid are 0/root , and Access is 0000 :

```
# stat /etc/shadow
Access: (0000/-) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set owner, group, and permissions on `/etc/shadow`:

```
# chown root:root /etc/shadow
# chmod 0000 /etc/shadow
```

Default Value:

Access: (0000/-) Uid: (0/ root) Gid: (0/ root)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.	●	●	●

6.1.5 Ensure permissions on /etc/shadow- are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/shadow-` file is used to store backup information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

It is critical to ensure that the `/etc/shadow-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command and verify `Uid is 0/root, Gid is 0/root and Access is 0000`:

```
# stat /etc/shadow-
Access: (0000/-) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set owner, group, and permissions on `/etc/shadow-`:

```
# chown root:root /etc/shadow-
# chmod 0000 /etc/shadow-
```

Default Value:

`Access: (0000/-) Uid: (0/ root) Gid: (0/ root)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.1.6 Ensure permissions on /etc/gshadow are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/gshadow` file is used to store the information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the `/etc/gshadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/gshadow` file (such as group administrators) could also be useful to subvert the group.

Audit:

Run the following command and verify `Uid is 0/root, Gid is 0/root and Access is 0000`:

```
# stat /etc/gshadow
Access: (0000/-) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set owner, group, and permissions on `/etc/gshadow`

```
# chown root:root /etc/gshadow
# chmod 0000 /etc/gshadow
```

Default Value:

Access: (0000/-) Uid: (0/ root) Gid: (0/ root)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.	●	●	●

6.1.7 Ensure permissions on /etc/gshadow- are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The /etc/gshadow- file is used to store backup information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

It is critical to ensure that the /etc/gshadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command and verify Uid is 0/root, Gid is 0/root or <gid>/shadow, and Access is 0000:

```
# stat /etc/gshadow-
Access: (0000/-) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set owner, group, and permissions on /etc/gshadow- :

```
# chown root:root /etc/gshadow-
# chmod 0000 /etc/gshadow-
```

Default Value:

Access: (0000/-) Uid: (0/ root) Gid: (0/ root)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.	●	●	●

6.1.8 Ensure permissions on /etc/group are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/group` file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

Rationale:

The `/etc/group` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` or more restrictive:

```
# stat /etc/group
Access: (0644/-rw-r--r--)  Uid: (    0/      root)  Gid: (    0/      root)
```

Remediation:

Run the following commands to set owner, group, and permissions on `/etc/group`:

```
# chown root:root /etc/group
# chmod u-x,g-wx,o-wx /etc/group
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.1.9 Ensure permissions on /etc/group- are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The /etc/group- file contains a backup list of all the valid groups defined in the system.

Rationale:

It is critical to ensure that the /etc/group- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` or more restrictive:

```
# stat /etc/group-
Access: (0644/-rw-----) Uid: ( 0/    root) Gid: ( 0/    root)
```

Remediation:

Run the following commands to set owner, group, and permissions on /etc/group-:

```
# chown root:root /etc/group-
# chmod u-x,go-wx /etc/group-
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	<u>16.4 Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.1.10 Ensure the root account is the only account that has unrestricted access to the operating system (Automated)

Profile Applicability:

- STIG

Description:

The root account must be the only account having unrestricted access to the operating system.

Rationale:

If an account other than root also has a User Identifier (UID) of "0", it has root authority, giving that account unrestricted access to the entire operating system. Multiple accounts with a UID of "0" afford an opportunity for potential intruders to guess a password for a privileged account.

Audit:

Check the system for duplicate UID "0" assignments with the following command:

```
# awk -F: '$3 == 0 {print $1}' /etc/passwd
```

If any accounts other than root have a UID of "0", this is a finding.

Remediation:

Change the UID of any account on the system, other than root, that has a UID of "0". If the account is associated with system commands or applications, the UID should be changed to one greater than "0" but less than "1000". Otherwise, assign a UID of greater than "1000" that has not already been assigned.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230534

Rule ID: SV-230534r627750_rule

STIG ID: RHEL-08-040200

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.1.11 Ensure no world writable files exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the `chmod(2)` man page for more information.

Rationale:

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

Audit:

Run the following command and verify no files are returned:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -0002
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -0002
```

Remediation:

Removing write access for the "other" category (`chmod o-w <filename>`) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	13 Data Protection Data Protection			

6.1.12 Ensure no unowned files or directories exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

Run the following command and verify no files are returned:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev  
-nouser
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -nouser
```

Remediation:

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	●	●	●

6.1.13 Ensure no ungrouped files or directories exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

Run the following command and verify no files are returned:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -nogroup
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -nogroup
```

Remediation:

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	●	●	●

6.1.14 Ensure all public directories are owned by root or a system account (Manual)

Profile Applicability:

- STIG

Description:

The operating system's public directories must be owned by root or a system account to prevent unauthorized and unintended information transferred via shared system resources.

Rationale:

Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Audit:

Check to see that all public directories are owned by root or a system account with the following command:

```
# find / -type d -perm -0002 -exec ls -lLd {} \;
drwxrwxrwx 7 root root 4096 Jul 26 11:19 /tmp
```

If any of the returned directories are not owned by root or a system account, this is a finding.

Remediation:

Configure all public directories to be owned by root or a system account to prevent unauthorized and unintended information transferred via shared system resources.

Set the owner of all public directories as root or a system account using the command, replace "[Public Directory]" with any directory path not owned by root or a system account:

```
# chown root [Public Directory]
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230242

Rule ID: SV-230242r627750_rule

STIG ID: RHEL-08-010180

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.15 Audit SUID executables (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SUID programs, but it is important to identify and review such programs to ensure they are legitimate.

Audit:

Run the following command to list SUID files:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -4000
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -4000
```

Remediation:

Ensure that no rogue SUID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.1.16 Audit SGID executables (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different md5 checksum than what from the package. This is an indication that the binary may have been replaced.

Audit:

Run the following command to list SGID files:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -2000
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -2000
```

Remediation:

Ensure that no rogue SGID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.1.17 Ensure the "/var/log/messages" file has mode "0640" or less permissive (Automated)

Profile Applicability:

- STIG

Description:

The "/var/log/messages" file must have mode "0640" or less permissive.

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the "/var/log/messages" file has mode "0640" or less permissive with the following command:

```
# stat -c "%a %n" /var/log/messages  
640 /var/log/messages
```

If a value of "0640" or less permissive is not returned, this is a finding.

Remediation:

Change the permissions of the file "/var/log/messages" to "0640" by running the following command:

```
# chmod 0640 /var/log/messages
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230245

Rule ID: SV-230245r627750_rule

STIG ID: RHEL-08-010210

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.18 Ensure the "/var/log/messages" file is owned by root (Automated)

Profile Applicability:

- STIG

Description:

The "/var/log/messages" file must be owned by root.

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the "/var/log/messages" file is owned by root with the following command:

```
# stat -c "%U" /var/log/messages
root
```

If "root" is not returned as a result, this is a finding.

Remediation:

Change the owner of the file /var/log/messages to root by running the following command:

```
# chown root /var/log/messages
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230246

Rule ID: SV-230246r627750_rule

STIG ID: RHEL-08-010220

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.19 Ensure the "/var/log/messages" file is group-owned by root (Automated)

Profile Applicability:

- STIG

Description:

The "/var/log/messages" file must be group-owned by root.

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the "/var/log/messages" file is group-owned by root with the following command:

```
# stat -c "%G" /var/log/messages
root
```

If "root" is not returned as a result, this is a finding.

Remediation:

Change the group of the file "/var/log/messages" to "root" by running the following command:

```
# chgrp root /var/log/messages
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230247

Rule ID: SV-230247r627750_rule

STIG ID: RHEL-08-010230

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.20 Ensure the "/var/log" directory has a mode of "0755" or less (Automated)

Profile Applicability:

- STIG

Description:

The "/var/log" directory must have mode 0755 or less permissive.

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the "/var/log" directory has a mode of "0755" or less with the following command:

```
# stat -c "%a %n" /var/log  
755
```

If a value of "0755" or less permissive is not returned, this is a finding.

Remediation:

Change the permissions of the directory "/var/log" to "0755" by running the following command:

```
# chmod 0755 /var/log
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230248

Rule ID: SV-230248r627750_rule

STIG ID: RHEL-08-010240

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.21 Ensure the "/var/log" directory is owned by root (Automated)

Profile Applicability:

- STIG

Description:

The "/var/log" directory must be owned by root.

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the "/var/log" directory is owned by root with the following command:

```
# stat -c "%U" /var/log
root
```

If "root" is not returned as a result, this is a finding.

Remediation:

Change the owner of the directory "/var/log" to root by running the following command:

```
# chown root /var/log
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230249

Rule ID: SV-230249r627750_rule

STIG ID: RHEL-08-010250

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.22 Ensure the "/var/log" directory is group-owned by root (Automated)

Profile Applicability:

- STIG

Description:

The "/var/log" directory must be group-owned by root.

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the "/var/log" directory is group-owned by root with the following command:

```
# stat -c "%G" /var/log
root
```

If "root" is not returned as a result, this is a finding.

Remediation:

Change the group of the directory "/var/log" to "root" by running the following command:

```
# chgrp root /var/log
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230250

Rule ID: SV-230250r627750_rule

STIG ID: RHEL-08-010260

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.23 Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories have mode "0755" or less permissive (Automated)

Profile Applicability:

- STIG

Description:

System commands must have mode "0755" or less permissive.

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands contained in the following directories have mode "0755" or less permissive with the following command:

```
# find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm /0022 -exec ls -l {} \;
```

If any system commands are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the system commands to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any system command with a mode more permissive than "0755".

```
# chmod 0755 [FILE]
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230257

Rule ID: SV-230257r627750_rule

STIG ID: RHEL-08-010300

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.24 Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are owned by "root" (Automated)

Profile Applicability:

- STIG

Description:

System commands must be owned by root.

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands contained in the following directories are owned by "root" with the following command:

```
# find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -  
user root -exec ls -l {} \;
```

If any system commands are returned, this is a finding.

Remediation:

Configure the system commands to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any system command file not owned by "root".

```
# chown root [FILE]
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230258

Rule ID: SV-230258r627750_rule

STIG ID: RHEL-08-010310

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.25 Ensure the system commands contained in "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are group-owned by "root" (Manual)

Profile Applicability:

- STIG

Description:

System commands must be group-owned by root or a system account.

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands contained in the following directories are group-owned by "root" with the following command:

```
# find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -  
group root -exec ls -l {} \;
```

If any system commands are returned and is not owned by a required system account, this is a finding.

Remediation:

Configure the system commands to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any system command file not group-owned by "root" or a required system account.

```
# chgrp root [FILE]
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230259

Rule ID: SV-230259r627750_rule

STIG ID: RHEL-08-010320

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.26 Ensure the system-wide shared library files contained in the "/lib, /lib64, /usr/lib, /usr/lib64" directories have mode "0755" or less permissive (Automated)

Profile Applicability:

- STIG

Description:

Library files must have mode "0755" or less permissive.

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library files contained in the following directories have mode "0755" or less permissive with the following command:

```
# find -L /lib /lib64 /usr/lib /usr/lib64 -perm /0022 -type f -exec ls -l {} \\;
```

If any system-wide shared library file is found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the library files to be protected from unauthorized access. Run the following command, replacing "[FILE]" with any library file with a mode more permissive than 0755.

```
# chmod 0755 [FILE]
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230260

Rule ID: SV-230260r627750_rule

STIG ID: RHEL-08-010330

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.27 Ensure the system-wide shared library files are owned by "root" (Automated)

Profile Applicability:

- STIG

Description:

Library files must be owned by root.

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library files are owned by "root" with the following command:

```
# find -L /lib /lib64 /usr/lib /usr/lib64 ! -user root -exec ls -l {} \;
```

If any system wide shared library file is returned, this is a finding.

Remediation:

Configure the system-wide shared library files (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any library file not owned by "root".

```
# chown root [FILE]
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230261

Rule ID: SV-230261r627750_rule

STIG ID: RHEL-08-010340

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.28 Ensure the system-wide shared library files are group-owned by "root" (Manual)

Profile Applicability:

- STIG

Description:

Library files must be group-owned by root or a system account.

Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library files are group-owned by "root" with the following command:

```
# find -L /lib /lib64 /usr/lib /usr/lib64 ! -group root -exec ls -l {} \;
```

If any system wide shared library file is returned and is not group-owned by a required system account, this is a finding.

Remediation:

Configure the system-wide shared library files (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any library file not group-owned by "root".

```
# chgrp root [FILE]
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230262

Rule ID: SV-230262r627750_rule

STIG ID: RHEL-08-010350

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.29 Ensure world-writable directories are owned by root, sys, bin, or an application user (Manual)

Profile Applicability:

- STIG

Description:

All world-writable directories must be owned by root, sys, bin, or an application user.

Rationale:

If a world-writable directory is not owned by root, sys, bin, or an application User Identifier (UID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Audit:

The following command will discover and print world-writable directories that are not owned by a system account, given the assumption that only system accounts have a UID lower than 1000. Run it once for each local partition [PART]:

```
# find [PART] -xdev -type d -perm -0002 -uid +999 -print
```

If there is output, this is a finding.

Remediation:

All directories in local partitions which are world-writable should be owned by root or another system account. If any world-writable directories are not owned by a system account, this should be investigated. Following this, the files should be deleted or assigned to an appropriate group.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230318

Rule ID: SV-230318r743960_rule

STIG ID: RHEL-08-010700

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.30 Ensure world-writable directories are group-owned by root, sys, bin, or an application group (Manual)

Profile Applicability:

- STIG

Description:

All world-writable directories must be group-owned by root, sys, bin, or an application group.

Rationale:

If a world-writable directory is not group-owned by root, sys, bin, or an application Group Identifier (GID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Audit:

The following command will discover and print world-writable directories that are not group-owned by a system account, given the assumption that only system accounts have a GID lower than 1000. Run it once for each local partition [PART]:

```
# find [PART] -xdev -type d -perm -0002 -gid +999 -print
```

If there is output, this is a finding.

Remediation:

All directories in local partitions which are world-writable must be group-owned by root or another system account. If any world-writable directories are not group-owned by a system account, this must be investigated. Following this, the directories must be deleted or assigned to an appropriate group.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230319

Rule ID: SV-230319r743961_rule

STIG ID: RHEL-08-010710

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.1.31 Ensure local initialization files do not execute world-writable programs (Manual)

Profile Applicability:

- STIG

Description:

Local operating system initialization files must not execute world-writable programs.

Rationale:

If user start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to destroy user files or otherwise compromise the system at the user level. If the system is compromised at the user level, it is easier to elevate privileges to eventually compromise the system at the root and network level.

Audit:

Verify that local initialization files do not execute world-writable programs.
Check the system for world-writable files.

The following command will discover and print world-writable files. Run it once for each local partition [PART]:

```
# find [PART] -xdev -type f -perm -0002 -print
```

For all files listed, check for their presence in the local initialization files with the following commands:

Note: The example will be for a system that is configured to create user home directories in the "/home" directory.

```
# grep <file> /home/*/*
```

If any local initialization files are found to reference world-writable files, this is a finding.

Remediation:

Set the mode on files being executed by the local initialization files with the following command:

```
# chmod 0755 <file>
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230309

Rule ID: SV-230309r627750_rule

STIG ID: RHEL-08-010660

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.1.32 Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer (Automated)

Profile Applicability:

- STIG

Description:

The operating system must ensure session control is automatically started at shell initialization.

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, the operating system needs to provide users with the ability to manually invoke a session lock so users can secure their session if it is necessary to temporarily vacate the immediate physical vicinity.

Tmux is a terminal multiplexer that enables a number of terminals to be created, accessed, and controlled from a single screen. Red Hat endorses tmux as the recommended session controlling package.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Verify the operating system shell initialization file is configured to start each shell with the tmux terminal multiplexer with the following command:

```
# grep -i tmux /etc/bashrc  
[ -n "$PS1" -a -z "$TMUX" ] && exec tmux
```

If "tmux" is not configured as the example above, is commented out, or missing from the "/etc/bashrc" initialization file, this is a finding.

Remediation:

Configure the operating system to initialize the tmux terminal multiplexer as each shell is called by adding the following line to the end of the "/etc/bashrc" configuration file:

```
[ -n "$PS1" -a -z "$TMUX" ] && exec tmux
```

This setting will take effect at next logon.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230349

Rule ID: SV-230349r627750_rule

STIG ID: RHEL-08-020041

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.1.33 Ensure the operating system prevents users from disabling the tmux terminal multiplexer (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent users from disabling session control mechanisms.

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, the operating system needs to provide users with the ability to manually invoke a session lock so users can secure their session if it is necessary to temporarily vacate the immediate physical vicinity.

Tmux is a terminal multiplexer that enables a number of terminals to be created, accessed, and controlled from a single screen. Red Hat endorses tmux as the recommended session controlling package.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Verify the operating system prevents users from disabling the tmux terminal multiplexer with the following command:

```
# grep -i tmux /etc/shells
```

If any output is produced, this is a finding.

Remediation:

Configure the operating system to prevent users from disabling the tmux terminal multiplexer by editing the "/etc/shells" configuration file to remove any instances of tmux.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230350

Rule ID: SV-230350r627750_rule

STIG ID: RHEL-08-020042

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.1.34 Ensure the operating system enables a user's session lock until that user re-establishes access (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures for graphical user sessions.

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Verify the operating system enables a user's session lock until that user re-establishes access using established identification and authentication procedures with the following command:

```
# gsettings get org.gnome.desktop.screensaver lock-enabled  
true
```

If the setting is "false", this is a finding.

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Remediation:

Configure the operating system to enable a user's session lock until that user re-establishes access using established identification and authentication procedures.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following example:

```
# vi /etc/dconf/db/local.d/00-screensaver
```

Edit the "[org/gnome/desktop/screensaver]" section of the database file and add or update the following lines:

```
# Set this to true to lock the screen when the screensaver activates  
lock-enabled=true
```

Update the system databases:

```
# dconf update
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230347

Rule ID: SV-230347r627750_rule

STIG ID: RHEL-08-020030

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

6.1.35 Ensure the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces (Automated)

Profile Applicability:

- STIG

Description:

The operating system must automatically lock graphical user sessions after 15 minutes of inactivity.

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, the operating system needs to provide users with the ability to manually invoke a session lock so users can secure their session if it is necessary to temporarily vacate the immediate physical vicinity.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012

Audit:

Verify the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces with the following commands:

This requirement assumes the use of the operating system's default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
# gsettings get org.gnome.desktop.session idle-delay  
uint32 900
```

If "idle-delay" is set to "0" or a value greater than "900", this is a finding.

Remediation:

Configure the operating system to initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

```
# touch /etc/dconf/db/local.d/00-screensaver
```

Edit /etc/dconf/db/local.d/00-screensaver and add or update the following lines:

```
[org/gnome/desktop/session]
# Set the lock time out to 900 seconds before the session is considered idle
idle-delay=uint32 900
```

Update the system databases:

```
# dconf update
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230352

Rule ID: SV-230352r646876_rule

STIG ID: RHEL-08-020060

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

6.1.36 Ensure the operating system initiates a session lock after 15 minutes of inactivity (Automated)

Profile Applicability:

- STIG

Description:

The operating system must automatically lock command line user sessions after 15 minutes of inactivity.

Rationale:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012

Audit:

Verify the operating system initiates a session lock after 15 minutes of inactivity.

Check the value of the system inactivity timeout with the following command:

```
# grep -i lock-after-time /etc/tmux.conf  
set -g lock-after-time 900
```

If "lock-after-time" is not set to "900" or less in the global tmux configuration file to enforce session lock after inactivity, this is a finding.

Remediation:

Configure the operating system to enforce session lock after a period of 15 minutes of inactivity by adding the following line to the "/etc/tmux.conf" global configuration file:

```
set -g lock-after-time 900
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230353

Rule ID: SV-230353r627750_rule

STIG ID: RHEL-08-020070

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

6.1.37 Ensure all accounts on the system are assigned to an active system, application, or user account (Manual)

Profile Applicability:

- STIG

Description:

The operating system must not have unnecessary accounts.

Rationale:

Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.

Audit:

Verify all accounts on the system are assigned to an active system, application, or user account.

Obtain the list of authorized system accounts from the Information System Security Officer (ISSO).

Check the system accounts on the system with the following command:

```
# more /etc/passwd

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
```

Accounts such as "games" and "gopher" are not authorized accounts as they do not support authorized system functions.

If the accounts on the system do not match the provided documentation, or accounts that do not support an authorized system function are present, this is a finding.

Remediation:

Configure the system so all accounts on the system are assigned to an active system, application, or user account.

Remove accounts that do not support approved system activities or that allow for a normal user to perform administrative-level actions.

Document all authorized accounts on the system.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230379

Rule ID: SV-230379r627750_rule

STIG ID: RHEL-08-020320

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.			

6.2 User and Group Settings

This section provides guidance on securing aspects of the users and groups.

Note: The recommendations in this section check local users and groups. Any users or groups from other sources such as LDAP will not be audited. In a domain environment similar checks should be performed against domain users and groups.

6.2.1 Ensure password fields are not empty (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

An account with an empty password field means that anybody may log in as that user without providing a password.

Rationale:

All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.

Audit:

Run the following command and verify that no output is returned:

```
# awk -F: '($2 == "") { print $1 " does not have a password "}' /etc/shadow
```

Remediation:

If any accounts in the `/etc/shadow` file do not have a password, run the following command to lock the account until it can be determined why it does not have a password:

```
# passwd -l <username>
```

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be forced off.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

6.2.2 Ensure no legacy "+" entries exist in /etc/passwd (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:

Run the following command and verify that no output is returned:

```
# grep -P '^+\+[^\n\r]*:' /etc/passwd
```

Remediation:

Remove any legacy '+' entries from /etc/passwd if they exist.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	●	●	●

6.2.3 Ensure root PATH Integrity (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `root` user can execute any command on the system and could be fooled into executing programs unintentionally if the `PATH` is not set correctly.

Rationale:

Including the current working directory (`.`) or other writable directory in `root`'s executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as `root` to execute a Trojan horse program.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

RPCV=$(sudo -Hiu root env | grep '^PATH=' | cut -d= -f2)
echo "$RPCV" | grep -q ":" && echo "root's path contains an empty directory (::)"
echo "$RPCV" | grep -q ":$" && echo "root's path contains a trailing (:)"
for x in $(echo "$RPCV" | tr ":" " "); do
    if [ -d "$x" ]; then
        ls -ldH "$x" | awk '$9 == "." {print "PATH contains current working
directory (.)}'
        $3 != "root" {print $9, "is not owned by root"}
        substr($1,6,1) != "-" {print $9, "is group writable"}
        substr($1,9,1) != "-" {print $9, "is world writable"}'
    else
        echo "$x is not a directory"
    fi
done
```

Remediation:

Correct or justify any items discovered in the Audit step.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.4 Ensure no legacy "+" entries exist in /etc/shadow (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:

Run the following command and verify that no output is returned:

```
# grep -P '^+\+[^\n\r]*:' /etc/shadow
```

Remediation:

Remove any legacy '+' entries from /etc/shadow if they exist.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	●	●	●

6.2.5 Ensure no legacy "+" entries exist in /etc/group (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:

Run the following command and verify that no output is returned:

```
# grep -P '^+\+[^\n\r]*:' /etc/group
```

Remediation:

Remove any legacy '+' entries from /etc/group if they exist.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	●	●	●

6.2.6 Ensure root is the only UID 0 account (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Any account with UID 0 has superuser privileges on the system.

Rationale:

This access must be limited to only the default `root` account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in recommendation "Ensure access to the `su` command is restricted".

Audit:

Run the following command and verify that only "root" is returned:

```
# awk -F: '($3 == 0) { print $1 }' /etc/passwd
root
```

Remediation:

Remove any users other than `root` with UID 0 or assign them a new UID if appropriate.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.7 Ensure users' home directories permissions are 750 or more restrictive (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

Rationale:

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\|/usr)?\|/sbin\|/nologin(\|/)?$/ && $7!~/(\|/usr)?\|/bin\|/false(\|/)?$/)
{print $1 " " $6}' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "User: \"\$user\" home directory: \"\$dir\" doesn't exist"
    else
        dirperm=$(stat -L -c "%A" "$dir")
        if [ "$(echo \"$dirperm\" | cut -c6)" != "-" ] || [ "$(echo \"$dirperm\" |
cut -c8)" != "-" ] || [ "$(echo \"$dirperm\" | cut -c9)" != "-" ] || [ "$(echo
=\"$dirperm\" | cut -c10)" != "-" ]; then
            echo "User: \"\$user\" home directory: \"\$dir\" has permissions:
\"$(stat -L -c "%a" "$dir")\""
        fi
    fi
done
```

Remediation:

Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

The following script can be used to remove permissions is excess of 750 from users' home directories:

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\|/usr)?\|/sbin\|/nologin(\|/)?$/ && $7!~^(\|/usr)?\|/bin\|/false(\|/)?$/) {
print $6}' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        dirperm=$(stat -L -c "%A" "$dir")
        if [ "$(echo "$dirperm" | cut -c6)" != "-" ] || [ "$(echo "$dirperm" |
cut -c8)" != "-" ] || [ "$(echo "$dirperm" | cut -c9)" != "-" ] || [ "$(echo
"$dirperm" | cut -c10)" != "-" ]; then
            chmod g-w,o-rwx "$dir"
        fi
    fi
done
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230321

Rule ID: SV-230321r627750_rule

STIG ID: RHEL-08-010730

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.2.8 Ensure emergency accounts have been provisioned with an expiration date of 72 hours (Manual)

Profile Applicability:

- STIG

Description:

Emergency accounts must be automatically removed or disabled after the crisis is resolved or within 72 hours.

Rationale:

Emergency accounts are privileged accounts established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are automatically disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Emergency accounts are different from infrequently used accounts (i.e., local logon accounts used by the organization's system administrators when network or normal logon/access is not available). Infrequently used accounts are not subject to automatic termination dates. Emergency accounts are accounts created in response to crisis situations, usually for use by maintenance personnel. The automatic expiration or disabling time period may be extended as needed until the crisis is resolved; however, it must not be extended indefinitely. A permanent account should be established for privileged users who need long-term maintenance accounts.

To address access requirements, many RHEL operating systems can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Audit:

Verify emergency accounts have been provisioned with an expiration date of 72 hours.

For every existing emergency account, run the following command to obtain its account expiration information.

```
# chage -l system_account_name
```

Verify each of these accounts has an expiration date set within 72 hours.

If any emergency accounts have no expiration date set or do not expire within 72 hours, this is a finding.

Remediation:

If an emergency account must be created, configure the system to terminate the account after 72 hours with the following command to set an expiration date for the account. Substitute "system_account_name" with the account to be created.

```
# chage -E `date -d "+3 days" +%Y-%m-%d` system_account_name
```

The automatic expiration or disabling time period may be extended as needed until the crisis is resolved.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230374

Rule ID: SV-230374r627750_rule

STIG ID: RHEL-08-020270

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.9 Ensure users own their home directories (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The user home directory is space defined for the particular user to set local environment variables and to store personal files.

Rationale:

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\!/usr)?\!/sbin\!/nologin(\!)?$/ && $7!~^(\!/usr)?\!/bin\!/false(\!)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "User: \"$user\" home directory: \"$dir\" does not exist."
    else
        owner=$(stat -L -c "%U" "$dir")
        if [ "$owner" != "$user" ]; then
            echo "User: \"$user\" home directory: \"$dir\" is owned by
\"$owner\""
        fi
    fi
done
```

Remediation:

Change the ownership of any home directories that are not owned by the defined user to the correct user.

The following script will create missing home directories, set the owner, and set the permissions for interactive users' home directories:

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~(^(\`/usr\`)?\`/sbin\`/nologin(\`/\`)?\$) && $7!~(^(\`/usr\`)?\`/bin\`/false(\`/\`)?\$)) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "User: \"\$user\" home directory: \"\$dir\" does not exist, creating
home directory"
        mkdir "$dir"
        chmod g-w,o-rwx "$dir"
        chown "$user" "$dir"
    else
        owner=$(stat -L -c "%U" "$dir")
        if [ "$owner" != "$user" ]; then
            chmod g-w,o-rwx "$dir"
            chown "$user" "$dir"
        fi
    fi
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.2.10 Ensure users' dot files are not group or world writable (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

Rationale:

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\!/usr)?\!/sbin?\!/nologin(\!)?$/ && $7!~^(\!/usr)?\!/bin?\!/false(\!)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ -d "$dir" ]; then
        for file in "$dir"/.*; do
            if [ ! -h "$file" ] && [ -f "$file" ]; then
                fileperm=$(stat -L -c "%A" "$file")
                if [ "$(echo "$fileperm" | cut -c6)" != "-" ] || [ "$(echo
"$fileperm" | cut -c9)" != "-" ]; then
                    echo "User: \"$user\" file: \"$file\" has permissions:
\"$fileperm\""
                fi
            done
        fi
    done
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.

The following script will remove excessive permissions on dot files within interactive users' home directories.

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\|/usr)?\|sbin\|nologin(\|)?$/ && $7!~^(\|/usr)?\|bin\|false(\|)?$/) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        for file in "$dir"/.*; do
            if [ ! -h "$file" ] && [ -f "$file" ]; then
                fileperm=$(stat -L -c "%A" "$file")
                if [ "$(echo "$fileperm" | cut -c6)" != "-" ] || [ "$(echo
"$fileperm" | cut -c9)" != "-" ]; then
                    chmod go-w "$file"
                fi
            fi
        done
    fi
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.2.11 Ensure no users have .forward files (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The .forward file specifies an email address to forward the user's mail to.

Rationale:

Use of the .forward file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The .forward file also poses a risk as it can be used to execute commands that may perform unintended actions.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '$1!~/^(root|halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\|/usr)?\|/sbin\|/nologin(\|/)?$/ && $7!~/(\|/usr)?\|/bin\|/false(\|/)?$/ {'
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
  if [ -d "$dir" ]; then
    file="$dir/.forward"
    if [ ! -h "$file" ] && [ -f "$file" ]; then
      echo "User: \"$user\" file: \"$file\" exists"
    fi
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

The following script will remove .forward files from interactive users' home directories

```
#!/bin/bash

awk -F: '$(1!~/^(root|halt|sync|shutdown|nobody) / &&
$7!~/^(\!/usr)?\!/sbin\!/nologin(\!)?$/ && $7!~^(\!/usr)?\!/bin\!/false(\!)?$/) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        file="$dir/.forward"
        [ ! -h "$file" ] && [ -f "$file" ] && rm -r "$file"
    fi
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.12 Ensure no users have .netrc files (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `.netrc` file contains data for logging into a remote host for file transfers via FTP.

Rationale:

The `.netrc` file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over `.netrc` files from other systems which could pose a risk to those systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '$1!~/^(root|halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\|/usr)?\|/sbin\|/nologin(\|/)?$/ && $7!~/(\|/usr)?\|/bin\|/false(\|/)?$/ {'
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
  if [ -d "$dir" ]; then
    file="$dir/.netrc"
    if [ ! -h "$file" ] && [ -f "$file" ]; then
      echo "User: \"$user\" file: \"$file\" exists"
    fi
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

The following script will remove .netrc files from interactive users' home directories

```
#!/bin/bash

awk -F: '$1!~/\(^(\halt|sync|shutdown|nfsnobody)\)/ &&
$7!~^(^(\usr)?\sbin\|nologin(\))?\$/ && $7!~/\(^(\usr)?\bin\|false(\))?\$/ {'
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        file="$dir/.netrc"
        [ ! -h "$file" ] && [ -f "$file" ] && rm -f "$file"
    fi
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.2.13 Ensure users' .netrc Files are not group or world accessible (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

While the system administrator can establish secure permissions for users' .netrc files, the users can easily override these.

Rationale:

The .netrc file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over .netrc files from other systems which could pose a risk to those systems.

If a .netrc file is required, and follows local site policy, it should have permissions of 600 or more restrictive.

Audit:

Run the following script. This script will return:

- FAILED: for any .netrc file with permissions less restrictive than 600
- WARNING: for any .netrc files that exist in interactive users' home directories.

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\|/usr)?\|sbin\|nologin(\|)?$/ && $7!~^(\|/usr)?\|bin\|/false(\|)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ -d "$dir" ]; then
        file="$dir/.netrc"
        if [ ! -h "$file" ] && [ -f "$file" ]; then
            if stat -L -c "%A" "$file" | cut -c4-10 | grep -Eq '[^-]+'; then
                echo "FAILED: User: \"$user\" file: \"$file\" exists with
permissions: \"$(stat -L -c "%a" "$file")\", remove file or excessive
permissions"
            else
                echo "WARNING: User: \"$user\" file: \"$file\" exists with
permissions: \"$(stat -L -c "%a" "$file")\", remove file unless required"
            fi
        fi
    fi
done
```

Verify:

- Any lines beginning with FAILED: - File should be removed unless deemed necessary, in accordance with local site policy, and permissions are updated to be 600 or more restrictive
- Any lines beginning with WARNING: - File should be removed unless deemed necessary, and in accordance with local site policy

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

The following script will remove .netrc files from interactive users' home directories

```
#!/bin/bash

awk -F: '$1!~/\((halt|sync|shutdown|nfsnobody)\) / &&
$7!~^(\|/usr)?\|/sbin?\|/nologin(\|/)?\$/ && $7!~/\|/usr)?\|/bin?\|/false(\|/)?\$/) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        file="$dir/.netrc"
        [ ! -h "$file" ] && [ -f "$file" ] && rm -f "$file"
    fi
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.2.14 Ensure no users have .rhosts files (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

While no .rhosts files are shipped by default, users can easily create them.

Rationale:

This action is only meaningful if .rhosts support is permitted in the file /etc/pam.conf. Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf, they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '$!~/^(root|halt|sync|shutdown|nfsnobody)/ &&
$!~/^(\!/usr)?\!/sbin?\!/nologin(\!)?$/ && $!~/^(\.?usr)?\!/bin?\!/false(\!)?$/ {'
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ -d "$dir" ]; then
        file="$dir/.rhosts"
        if [ ! -h "$file" ] && [ -f "$file" ]; then
            echo "User: \"$user\" file: \"$file\" exists"
        fi
    fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .rhosts files and determine the action to be taken in accordance with site policy.

The following script will remove .rhosts files from interactive users' home directories

```
#!/bin/bash

awk -F: '$(1!~/^(root|halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\!/usr)?\!/sbin?\!/nologin(\!)?$/ && $7!~^(\!/usr)?\!/bin?\!/false(\!)?$/) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        file="$dir/.rhosts"
        [ ! -h "$file" ] && [ -f "$file" ] && rm -r "$file"
    fi
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.2.15 Ensure all groups in /etc/passwd exist in /etc/group (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Over time, system administration errors and changes can lead to groups being defined in /etc/passwd but not in /etc/group.

Rationale:

Groups defined in the /etc/passwd file but not in the /etc/group file pose a threat to system security since group permissions are not properly managed.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

for i in $(cut -s -d: -f4 /etc/passwd | sort -u); do
    grep -q -P "^.+?:[^:]*:$i:" /etc/group
    if [ $? -ne 0 ]; then
        echo "Group $i is referenced by /etc/passwd but does not exist in
/etc/group"
    fi
done
```

Remediation:

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

6.2.16 Ensure no duplicate UIDs exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

Description:

Although the `useradd` program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the `/etc/passwd` file and change the UID field.

Rationale:

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -f3 -d":" /etc/passwd | sort -n | uniq -c | while read x ; do
    [ -z "$x" ] && break
    set - $x
    if [ $1 -gt 1 ] ; then
        users=$(awk -F: '$(3 == n) { print $1 }' n=$2 /etc/passwd | xargs)
        echo "Duplicate UID ($2): $users"
    fi
done
```

Remediation:

Based on the results of the audit script, establish unique UIDs and review all files owned by the shared UIDs to determine which UID they are supposed to belong to.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230371

Rule ID: SV-230371r627750_rule

STIG ID: RHEL-08-020240

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	16 Account Monitoring and Control Account Monitoring and Control			

6.2.17 Ensure no duplicate GIDs exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Although the `groupadd` program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the `/etc/group` file and change the GID field.

Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -d: -f3 /etc/group | sort | uniq -d | while read x ; do
    echo "Duplicate GID ($x) in /etc/group"
done
```

Remediation:

Based on the results of the audit script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

Additional Information:

You can also use the `grpck` command to check for other inconsistencies in the `/etc/group` file.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

6.2.18 Ensure no duplicate user names exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Although the `useradd` program will not let you create a duplicate user name, it is possible for an administrator to manually edit the `/etc/passwd` file and change the user name.

Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in `/etc/passwd`. For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000.

Effectively, the UID is shared, which is a security problem.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -d: -f1 /etc/passwd | sort | uniq -d | while read x; do
    echo "Duplicate login name ${x} in /etc/passwd"
done
```

Remediation:

Based on the results of the audit script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

6.2.19 Ensure no duplicate group names exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Although the `groupadd` program will not let you create a duplicate group name, it is possible for an administrator to manually edit the `/etc/group` file and change the group name.

Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in `/etc/group`. Effectively, the GID is shared, which is a security problem.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -d: -f1 /etc/group | sort | uniq -d | while read -r x; do
    echo "Duplicate group name ${x} in /etc/group"
done
```

Remediation:

Based on the results of the audit script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

6.2.20 Ensure shadow group is empty (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The shadow group allows system programs which require access the ability to read the /etc/shadow file. No users should be assigned to the shadow group.

Rationale:

Any users assigned to the shadow group would be granted read access to the /etc/shadow file. If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert additional user accounts.

Audit:

Run the following commands and verify no results are returned:

```
# awk -F: '($1=="shadow") {print $NF}' /etc/group  
# awk -F: -v GID=$(awk -F: '($1=="shadow") {print $3}' /etc/group) "  
'($4==GID) {print $1}' /etc/passwd
```

Remediation:

Run the following command to remove all users from the shadow group

```
# sed -ri 's/^(shadow:[^:]*)*:[^:]*(:[^:]*)*$/\1/' /etc/group
```

Change the primary group of any users with shadow as their primary group.

```
# usermod -g <primary group> <user>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.21 Ensure all users' home directories exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Users can be defined in `/etc/passwd` without a home directory or with a home directory that does not actually exist.

Rationale:

If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\|usr)?\|sbin\|nologin(\|)?$/ && $7!~^(\|usr)?\|bin\|false(\|)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "User: \"$user\" home directory: \"$dir\" does not exist."
    fi
done
```

Note: The audit script checks all users with interactive shells except halt, sync, shutdown, and nfsnobody.

Remediation:

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

The following script will create a home directory for users with an interactive shell whose home directory doesn't exist:

```
#!/bin/bash

awk -F: '($1!~/\(\|halt|sync|shutdown|nfsnobody\)/ &&
$7!~^(\|usr\|)\|sbin\|nologin\(\)?)$/ && $7!~\(\|usr\|)\|bin\|false\(\)?)$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        mkdir "$dir"
        chmod g-w,o-wrx "$dir"
        chown "$user" "$dir"
    fi
done
```

Additional Information:

The audit script checks all users with interactive shells except halt, sync, shutdown, and nfsnobody.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.22 Ensure the assigned home directory of all local interactive users is group-owned by that user's primary GID (Automated)

Profile Applicability:

- STIG

Description:

All local interactive user home directories must be group-owned by the home directory owner's primary group.

Rationale:

If the Group Identifier (GID) of a local interactive user's home directory is not the same as the primary GID of the user, this would allow unauthorized access to the user's files, and users that share the same group may not be able to access files that they legitimately should.

Audit:

Verify the assigned home directory of all local interactive users is group-owned by that user's primary GID with the following command:

Note: This may miss local interactive users that have been assigned a privileged UID. Evidence of interactive use may be obtained from a number of log files containing system logon information. The returned directory "/home.smithj" is used as an example.

```
# ls -ld $(awk -F: '$(3>=1000)&&($7 !~ /nologin/){print $6}' /etc/passwd)
drwxr-x--- 2 smithj admin 4096 Jun 5 12:41 smithj
```

Check the user's primary group with the following command:

```
# grep $(grep smithj /etc/passwd | awk -F: '{print $4}') /etc/group
admin:x:250:smithj,jonesj,jacksons
```

If the user home directory referenced in "/etc/passwd" is not group-owned by that user's primary GID, this is a finding.

Remediation:

Change the group owner of a local interactive user's home directory to the group found in "/etc/passwd". To change the group owner of a local interactive user's home directory, use the following command:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj", and has a primary group of users.

```
# chgrp users /home/smithj
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230322

Rule ID: SV-230322r743963_rule

STIG ID: RHEL-08-010740

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.2.23 Ensure the assigned home directory of all local interactive users exists (Automated)

Profile Applicability:

- STIG

Description:

All local interactive user home directories defined in the "/etc/passwd" file must exist.

Rationale:

If a local interactive user has a home directory defined that does not exist, the user may be given access to the "/" directory as the current working directory upon logon. This could create a denial of service because the user would not be able to access their logon configuration files, and it may give them visibility to system files they normally would not be able to access.

Audit:

Verify the assigned home directory of all local interactive users on RHEL 8 exists with the following command:

```
# ls -ld $(awk -F: '$(3>=1000) && ($7 !~ /nologin/) {print $6}' /etc/passwd)
drwxr-xr-x 2 smithj admin 4096 Jun 5 12:41 smithj
```

Note: This may miss interactive users that have been assigned a privileged User ID (UID). Evidence of interactive use may be obtained from a number of log files containing system logon information.

Check that all referenced home directories exist with the following command:

```
# pwck -r
user 'smithj': directory '/home/smithj' does not exist
```

If any home directories referenced in "/etc/passwd" are returned as not defined, this is a finding.

Remediation:

Create home directories to all local interactive users that currently do not have a home directory assigned. Use the following commands to create the user home directory assigned in "/etc/passwd":

Note: The example will be for the user smithj, who has a home directory of "/home/smithj", a UID of "smithj", and a Group Identifier (GID) of "users assigned" in "/etc/passwd".

```
# mkdir /home/smithj  
# chown smithj /home/smithj  
# chgrp users /home/smithj  
# chmod 0750 /home/smithj
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230323

Rule ID: SV-230323r627750_rule

STIG ID: RHEL-08-010750

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.24 Ensure all local interactive users are assigned a home directory upon creation (Automated)

Profile Applicability:

- STIG

Description:

All local interactive user accounts must be assigned a home directory upon creation.

Rationale:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Audit:

Verify all local interactive users are assigned a home directory upon creation with the following command:

```
# grep -i create_home /etc/login.defs  
CREATE_HOME yes
```

If the value for "CREATE_HOME" parameter is not set to "yes", the line is missing, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to assign home directories to all new local interactive users by setting the "CREATE_HOME" parameter in "/etc/login.defs" to "yes" as follows.

```
CREATE_HOME yes
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230324

Rule ID: SV-230324r627750_rule

STIG ID: RHEL-08-010760

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.25 Ensure all local initialization files have a mode of "0740" or less permissive (Automated)

Profile Applicability:

- STIG

Description:

All local initialization files must have mode "0740" or less permissive.

Rationale:

Local initialization files are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Audit:

Verify that all local initialization files have a mode of "0740" or less permissive with the following command:

Note: The example will be for the "smithj" user, who has a home directory of "/home/smithj".

```
# ls -al /home/smithj/.[^.]* | more
-rwxr-xr-x 1 smithj users 896 Mar 10 2011 .profile
-rwxr-xr-x 1 smithj users 497 Jan 6 2007 .login
-rwxr-xr-x 1 smithj users 886 Jan 6 2007 .something
```

If any local initialization files have a mode more permissive than "0740", this is a finding.

Remediation:

Set the mode of the local initialization files to "0740" with the following command:

Note: The example will be for the smithj user, who has a home directory of "/home/smithj".

```
# chmod 0740 /home/smithj/.<INIT_FILE>
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230325

Rule ID: SV-230325r627750_rule

STIG ID: RHEL-08-010770

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.2.26 Ensure all local files and directories have a valid owner (Automated)

Profile Applicability:

- STIG

Description:

All local files and directories must have a valid owner.

Rationale:

Unowned files and directories may be unintentionally inherited if a user is assigned the same User Identifier "UID" as the UID of the un-owned files.

Audit:

Verify all local files and directories have a valid owner with the following command:

Note: The value after -fstype must be replaced with the filesystem type. XFS is used as an example.

```
# find / -fstype xfs -nouser
```

If any files on the system do not have an assigned owner, this is a finding.

Note: Command may produce error messages from the /proc and /sys directories.

Remediation:

Either remove all files and directories from the system that do not have a valid user, or assign a valid user to all unowned files and directories on RHEL 8 with the "chown" command:

```
# chown <user> <file>
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230326

Rule ID: SV-230326r627750_rule

STIG ID: RHEL-08-010780

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	●	●	●

6.2.27 Ensure all local files and directories have a valid group (Automated)

Profile Applicability:

- STIG

Description:

All local files and directories must have a valid group owner.

Rationale:

Files without a valid group owner may be unintentionally inherited if a group is assigned the same Group Identifier (GID) as the GID of the files without a valid group owner.

Audit:

Verify all local files and directories on RHEL 8 have a valid group with the following command:

Note: The value after -fstype must be replaced with the filesystem type. XFS is used as an example.

```
# find / -fstype xfs -nogroup
```

If any files on the system do not have an assigned group, this is a finding.

Note: Command may produce error messages from the /proc and /sys directories.

Remediation:

Either remove all files and directories from RHEL 8 that do not have a valid group, or assign a valid group to all files and directories on the system with the "chgrp" command:

```
# chgrp <group> <file>
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230327

Rule ID: SV-230327r627750_rule

STIG ID: RHEL-08-010790

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	●	●	●

6.2.28 Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file (Manual)

Profile Applicability:

- STIG

Description:

The operating system must map the authenticated identity to the user or group account for PKI-based authentication.

Rationale:

Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

There are various methods of mapping certificates to user/group accounts. For the purposes of this requirement, the check and fix will account for Active Directory mapping. Some of the other possible methods include joining the system to a domain and utilizing a Red Hat idM server, or a local system mapping, where the system is not part of a domain.

Audit:

Verify the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file with the following command:

```
# cat /etc/sssd/sssd.conf

[sssd]
config_file_version = 2
services = pam, sudo, ssh
domains = testing.test

[pam]
pam_cert_auth = True

[domain/testing.test]
id_provider = ldap

[certmap/testing.test/rule_name]
matchrule = <SAN>.*EDIP@mil
maprule = (userCertificate;binary={cert!bin})
domains = testing.test
```

If the certmap section does not exist, ask the System Administrator to indicate how certificates are mapped to accounts. If there is no evidence of certificate mapping, this is a finding.

Remediation:

Configure the operating system to map the authenticated identity to the user or group account by adding or modifying the certmap section of the "/etc/sssd/sssd.conf" file based on the following example:

```
[certmap/testing.test/rule_name]
matchrule =<SAN>.*EDIPI@mil
maprule = (userCertificate;binary={cert!bin})
domains = testing.test
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230355

Rule ID: SV-230355r627750_rule

STIG ID: RHEL-08-020090

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.29 Ensure file executable search path statements do not share sensitive home directory information (Manual)

Profile Applicability:

- STIG

Description:

Executable search paths within the initialization files of all local interactive operating system users must only contain paths that resolve to the system default or the users home directory.

Rationale:

The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory (other than the user's home directory), executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. If deviations from the default system search path for the local interactive user are required, they must be documented with the Information System Security Officer (ISSO).

Audit:

Verify that all local interactive user initialization file executable search path statements do not contain statements that will reference a working directory other than user home directories with the following commands:

```
# grep -i path /home/*/.*
/home/[localinteractiveuser]/.bash_profile:PATH=$PATH:$HOME/.local/bin:$HOME/
bin
/home/[localinteractiveuser]/.bash_profile:export PATH
```

If any local interactive user initialization files have executable search path statements that include directories outside of their home directory and is not documented with the ISSO as an operational requirement, this is a finding.

Remediation:

Edit the local interactive user initialization files to change any PATH variable statements that reference directories other than their home directory.

If a local interactive user requires path variables to reference a directory owned by the application, it must be documented with the ISSO.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230317

Rule ID: SV-230317r627750_rule

STIG ID: RHEL-08-010690

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.30 Ensure local interactive users have a home directory assigned (Automated)

Profile Applicability:

- STIG

Description:

All local interactive users must have a home directory assigned in the "/etc/passwd" file.

Rationale:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Audit:

Verify local interactive users have a home directory assigned with the following command:

```
# pwck -r  
  
user 'lp': directory '/var/spool/lpd' does not exist  
user 'news': directory '/var/spool/news' does not exist  
user 'uucp': directory '/var/spool/uucp' does not exist  
user 'www-data': directory '/var/www' does not exist
```

Ask the System Administrator (SA) if any users found without home directories are local interactive users. If the SA is unable to provide a response, check for users with a User Identifier (UID) of 1000 or greater with the following command:

```
# awk -F: '($3>=1000)&&($7 !~ /nologin/){print $1, $3, $6}' /etc/passwd
```

If any interactive users do not have a home directory assigned, this is a finding.

Remediation:

Assign home directories to all local interactive users that currently do not have a home directory assigned.

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230320

Rule ID: SV-230320r627750_rule

STIG ID: RHEL-08-010720

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.31 Ensure the operating system limits the number of concurrent sessions to "10" for all accounts and/or account types (Automated)

Profile Applicability:

- STIG

Description:

The operating system must limit the number of concurrent sessions to ten for all accounts and/or account types.

Rationale:

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Audit:

Verify the operating system limits the number of concurrent sessions to "10" for all accounts and/or account types by issuing the following command:

```
# grep -r -s '^[^#].*maxlogins' /etc/security/limits.conf  
/etc/security/limits.d/*.conf  
  
* hard maxlogins 10
```

This can be set as a global domain (with the * wildcard) but may be set differently for multiple domains.

If the "maxlogins" item is missing, commented out, or the value is set greater than "10" and is not documented with the Information System Security Officer (ISSO) as an operational requirement for all domains that have the "maxlogins" item assigned, this is a finding.

Remediation:

Configure the operating system to limit the number of concurrent sessions to "10" for all accounts and/or account types.

Add the following line to the top of the "/etc/security/limits.conf" or in a ".conf" file defined in "/etc/security/limits.d/":

```
* hard maxlogins 10
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230346

Rule ID: SV-230346r627750_rule

STIG ID: RHEL-08-020024

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.32 Ensure the operating system enables a user's session lock until that user re-establishes access (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures for graphical user sessions.

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Verify the operating system enables a user's session lock until that user re-establishes access using established identification and authentication procedures with the following command:

```
# gsettings get org.gnome.desktop.screensaver lock-enabled  
true
```

If the setting is "false", this is a finding.

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Remediation:

Configure the operating system to enable a user's session lock until that user re-establishes access using established identification and authentication procedures.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following example:

```
# vi /etc/dconf/db/local.d/00-screensaver
```

Edit the "[org/gnome/desktop/screensaver]" section of the database file and add or update the following lines:

```
# Set this to true to lock the screen when the screensaver activates  
lock-enabled=true
```

Update the system databases:

```
# dconf update
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230347

Rule ID: SV-230347r627750_rule

STIG ID: RHEL-08-020030

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

6.2.33 Ensure the operating system enables the user to initiate a session lock (Automated)

Profile Applicability:

- STIG

Description:

The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures for command line sessions.

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, the operating system needs to provide users with the ability to manually invoke a session lock so users can secure their session if it is necessary to temporarily vacate the immediate physical vicinity.

Tmux is a terminal multiplexer that enables a number of terminals to be created, accessed, and controlled from a single screen. Red Hat endorses tmux as the recommended session controlling package.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Verify the operating system enables the user to initiate a session lock with the following command:

```
# grep -i lock-command /etc/tmux.conf  
set -g lock-command vlock
```

If the "lock-command" is not set in the global settings to call "vlock", this is a finding.

Remediation:

Configure the operating system to enable a user to initiate a session lock via tmux. Create a global configuration file "/etc/tmux.conf" and add the following line:

```
set -g lock-command vlock
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230348

Rule ID: SV-230348r743987_rule

STIG ID: RHEL-08-020040

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

6.2.34 Ensure the operating system prevents a user from overriding settings for graphical user interfaces (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent a user from overriding the session lock-delay setting for the graphical user interface.

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Implementing session settings will have little value if a user is able to manipulate these settings from the defaults prescribed in the other requirements of this implementation guide.

Locking these settings from non-privileged users is crucial to maintaining a protected baseline.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012, SRG-OS-000480-GPOS-00227

Audit:

Verify the operating system prevents a user from overriding settings for graphical user interfaces.

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user  
system-db:local
```

Check that graphical settings are locked from non-privileged user modification with the following command:

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
# grep -i lock-delay /etc/dconf/db/local.d/locks/*  
/org/gnome/desktop/screensaver/lock-delay
```

If the command does not return at least the example result, this is a finding.

Remediation:

Configure the operating system to prevent a user from overriding settings for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the following setting to prevent non-privileged users from modifying it:

```
/org/gnome/desktop/screensaver/lock-delay
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230354

Rule ID: SV-230354r743990_rule

STIG ID: RHEL-08-020080

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.35 Ensure all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750" (Automated)

Profile Applicability:

- STIG

Description:

All local interactive user home directory files must have mode "0750" or less permissive.

Rationale:

Excessive permissions on local interactive user home directories may allow unauthorized access to user files by other users.

Audit:

Verify all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750".

Files that begin with a "." are excluded from this requirement.

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

```
# ls -lLR /home/smithj
-rwxr-x--- 1 smithj smithj 18 Mar 5 17:06 file1
-rwxr----- 1 smithj smithj 193 Mar 5 17:06 file2
-rw-r-x--- 1 smithj smithj 231 Mar 5 17:06 file3
```

If any files or directories are found with a mode more permissive than "0750", this is a finding.

Remediation:

Set the mode on files and directories in the local interactive user home directory with the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj" and is a member of the users group.

```
# chmod 0750 /home/smithj/<file or directory>
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244531

Rule ID: SV-244531r743842_rule

STIG ID: RHEL-08-010731

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.2.36 Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that all files and directories contained in local interactive user home directories are group-owned by a group of which the home directory owner is a member.

Rationale:

If a local interactive user's files are group-owned by a group of which the user is not a member, unintended users may be able to access them.

Audit:

Verify all files and directories in a local interactive user home directory are group-owned by a group that the user is a member of.

Check the group owner of all files and directories in a local interactive user's home directory with the following command:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

```
# ls -lLR /<home directory>/<users home directory>/
-rw-r--r-- 1 smithj smithj 18 Mar 5 17:06 file1
-rw-r--r-- 1 smithj smithj 193 Mar 5 17:06 file2
-rw-r--r-- 1 smithj sa 231 Mar 5 17:06 file3
```

If any files found with a group-owner different from the home directory user private group, check to see if the user is a member of that group with the following command:

```
# grep smithj /etc/group
sa:x:100:juan,shelley,bob,smithj
smithj:x:521:smithj
```

If any files or directories are group owned by a group that the directory owner is not a member of, this is a finding.

Remediation:

Change the group of a local interactive user's files and directories to a group that the interactive user is a member. To change the group owner of a local interactive user's files and directories, use the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj" and is a member of the users group.

```
# chgrp smithj /home/smithj/<file or directory>
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244532

Rule ID: SV-244532r743845_rule

STIG ID: RHEL-08-010741

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

6.2.37 Ensure temporary accounts have been provisioned with an expiration date of 72 hours (Manual)

Profile Applicability:

- STIG

Description:

Temporary user accounts must be provisioned with an expiration time of 72 hours or less.

Rationale:

If temporary user accounts remain active when no longer needed or for an excessive period, these accounts may be used to gain unauthorized access. To mitigate this risk, automated termination of all temporary accounts must be set upon account creation.

Temporary accounts are established as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation.

If temporary accounts are used, the operating system must be configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours.

To address access requirements, many RHEL 8 operating systems may be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Audit:

Verify that temporary accounts have been provisioned with an expiration date of 72 hours.

For every existing temporary account, run the following command to obtain its account expiration information.

```
# chage -l system_account_name
```

Verify each of these accounts has an expiration date set within 72 hours.

If any temporary accounts have no expiration date set or do not expire within 72 hours, this is a finding.

Remediation:

If a temporary account must be created configure the system to terminate the account after a 72 hour time period with the following command to set an expiration date on it.

Substitute "system_account_name" with the account to be created.

```
# chage -E `date -d "+3 days" +%Y-%m-%d` system_account_name
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230331

Rule ID: SV-230331r627750_rule

STIG ID: RHEL-08-020000

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.3 Ensure the operating system removes all software components after updated versions have been installed (Automated)

Profile Applicability:

- STIG

Description:

DNF must remove all software components after updated versions have been installed on the operating system.

Rationale:

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Audit:

Verify the operating system removes all software components after updated versions have been installed.

Check if DNF is configured to remove unneeded packages with the following command:

```
# grep -i clean_requirements_on_remove /etc/dnf/dnf.conf  
clean_requirements_on_remove=True
```

If "clean_requirements_on_remove" is not set to either "1", "True", or "yes", commented out, or is missing from "/etc/dnf/dnf.conf", this is a finding.

Remediation:

Configure the operating system to remove all software components after updated versions have been installed.

Set the "clean_requirements_on_remove" option to "True" in the "/etc/dnf/dnf.conf" file:

```
clean_requirements_on_remove=True
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230281

Rule ID: SV-230281r627750_rule

STIG ID: RHEL-08-010440

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.4 Ensure there are no ".shosts" files on the operating system (Automated)

Profile Applicability:

- STIG

Description:

There must be no .shosts files on the operating system.

Rationale:

The ".shosts" files are used to configure host-based authentication for individual users or the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Audit:

Verify there are no ".shosts" files on the operating system with the following command:

```
# find / -name '*.shosts'
```

If any ".shosts" files are found, this is a finding.

Remediation:

Remove any found ".shosts" files from the system.

```
# rm /[path]/[to]/[file]/*.shosts
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230284

Rule ID: SV-230284r627750_rule

STIG ID: RHEL-08-010470

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.5 Ensure there are no "shosts.equiv" files on the operating system (Automated)

Profile Applicability:

- STIG

Description:

There must be no shosts.equiv files on the operating system.

Rationale:

The "shosts.equiv" files are used to configure host-based authentication for the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Audit:

Verify there are no "shosts.equiv" files on the operating with the following command:

```
# find / -name shosts.equiv
```

If a "shosts.equiv" file is found, this is a finding.

Remediation:

Remove any found "shosts.equiv" files from the system.

```
# rm /etc/ssh/shosts.equiv
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-230283

Rule ID: SV-230283r627750_rule

STIG ID: RHEL-08-010460

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

Appendix: Recommendation Summary Table

Control		Set Correctly	
		Yes	No
1	Initial Setup		
1.1	Filesystem Configuration		
1.1.1	Disable unused filesystems		
1.1.1.1	Ensure mounting of cramfs filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure mounting of vFAT filesystems is limited (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure mounting of squashfs filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure mounting of udf filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Ensure /tmp is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Ensure nodev option set on /tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Ensure nosuid option set on /tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Ensure noexec option set on /tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	Ensure separate partition exists for /var (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Ensure separate partition exists for /var/tmp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Ensure nodev option set on /var/tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Ensure nosuid option set on /var/tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Ensure noexec option set on /var/tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.11	Ensure separate partition exists for /var/log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.12	Ensure separate partition exists for /var/log/audit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.13	Ensure separate partition exists for /home (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.14	Ensure nodev option set on /home partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.15	Ensure nodev option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.16	Ensure nosuid option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.17	Ensure noexec option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.18	Ensure nodev option set on removable media partitions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.19	Ensure nosuid option set on removable media partitions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.20	Ensure noexec option set on removable media partitions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

1.1.21	Ensure sticky bit is set on all world-writable directories (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.22	Disable Automounting (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.23	Disable USB Storage (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.24	Ensure file systems that contain user home directories are mounted with the "nosuid" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.25	Ensure the "/boot" directory is mounted with the "nosuid" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.26	Ensure all non-root local partitions are mounted with the "nodev" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.27	Ensure file systems that are being NFS-imported are mounted with the "nodev" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.28	Ensure file systems being imported via NFS are mounted with the "noexec" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.29	Ensure file systems being imported via NFS are mounted with the "nosuid" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.30	Ensure a separate file system/partition has been created for non-privileged local interactive user home directories (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.31	Ensure "/var/log" is mounted with the "nodev" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.32	Ensure "/var/log" is mounted with the "nosuid" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.33	Ensure "/var/log" is mounted with the "noexec" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.34	Ensure "/var/log/audit" is mounted with the "nodev" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.35	Ensure "/var/log/audit" is mounted with the "nosuid" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.36	Ensure "/var/log/audit" is mounted with the "noexec" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.37	Ensure the "/boot/efi" directory is mounted with the "nosuid" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.38	Ensure file systems that contain user home directories are mounted with the "noexec" option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Configure Software Updates		
1.2.1	Ensure GPG keys are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Ensure gpgcheck is globally activated (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Ensure package manager repositories are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Ensure DNF is configured to perform a signature check on local packages (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Configure sudo		
1.3.1	Ensure sudo is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Ensure sudo commands use pty (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

1.3.3	Ensure sudo log file exists (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Ensure the "/etc/sudoers" file has no occurrences of "NOPASSWD" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	Ensure the "/etc/sudoers" file has no occurrences of "!authenticate" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.6	Ensure the "sudoers" file restricts sudo access to authorized personnel (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.7	Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.8	Ensure the operating system requires re-authentication when using the "sudo" command to elevate privileges (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	Filesystem Integrity Checking		
1.4.1	Ensure AIDE is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure filesystem integrity is regularly checked (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Ensure Advanced Intrusion Detection Environment (AIDE) is properly configured to use cryptographic mechanisms to protect the integrity of audit tools (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.4	Ensure the file integrity tool is configured to verify extended attributes (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.5	Ensure the file integrity tool is configured to verify ACLs (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Secure Boot Settings		
1.5.1	Ensure permissions on bootloader config are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure bootloader password is set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Ensure authentication required for single user mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Ensure the encrypted grub superusers password is set for systems booted with UEFI (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Ensure the encrypted grub superusers password is set for system booted with BIOS (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.6	Ensure the operating system requires authentication for rescue mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.7	Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.8	Ensure GRUB 2 is configured to disable vsyscalls (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.9	Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.10	Ensure the operating system is configured to boot to the command line (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

1.5.11	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.12	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.13	Ensure a unique name is set as the "superusers" account (UEFI) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.14	Ensure a unique name is set as the "superusers" account (BIOS) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.15	Ensure the operating system requires authentication upon booting into emergency mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Additional Process Hardening		
1.6.1	Ensure core dumps are restricted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.2	Ensure address space layout randomization (ASLR) is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.3	Ensure the operating system disables the storing core dumps (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure the operating system is not configured to acquire, save, or process core dumps (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure kernel core dumps are disabled unless needed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure the operating system disables core dumps for all users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.7	Ensure the operating system disables storing core dumps for all users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.8	Ensure the operating system disables core dump backtraces (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Mandatory Access Control		
1.7.1	Configure SELinux		
1.7.1.1	Ensure SELinux is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.2	Ensure SELinux is not disabled in bootloader configuration (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.3	Ensure SELinux policy is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.4	Ensure the SELinux state is enforcing (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.5	Ensure no unconfined services exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.6	Ensure SETroubleshoot is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.7	Ensure the MCS Translation Service (mcstrans) is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.8	Ensure the operating system has the policycoreutils package installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Command Line Warning Banners		
1.8.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

1.8.2	Ensure message of the day is configured properly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.3	Ensure local login warning banner is configured properly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.4	Ensure remote login warning banner is configured properly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.5	Ensure permissions on /etc/motd are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.6	Ensure permissions on /etc/issue are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.7	Ensure permissions on /etc/issue.net are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.8	Ensure the Standard Mandatory DoD Notice and Consent Banner is displayed before granting access to the system via SSH logon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.9	Ensure the operating system displays a banner before granting access to the operating system via a graphical user logon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9	GNOME Display Manager		
1.9.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9.2	Ensure GNOME Display Manager is removed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.9.3	Ensure GDM login banner is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9.4	Ensure last logged in user display is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9.5	Ensure XDCMP is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9.6	Ensure a Standard Mandatory DoD Notice and Consent Banner is displayed via a graphical user logon (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.9.7	Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9.8	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9.9	Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9.10	Ensure the operating system disables the user logon list for graphical user interfaces (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9.11	Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9.12	Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

1.10	Ensure updates, patches, and additional security software are installed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure system-wide crypto policy is not legacy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.12	Ensure system-wide crypto policy is FUTURE or FIPS (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.13	Ensure the operating system implements DoD-approved encryption (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.14	Ensure the operating system prevents unauthorized modification of all information at rest by using disk encryption (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.15	Ensure kernel image loading is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure the operating system is configured to enable DAC on symlinks (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.17	Ensure the operating system is configured to enable DAC on hardlinks (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.18	Ensure the operating system is configured to restrict access to the kernel message buffer (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.19	Ensure the operating system is configured to prevent kernel profiling by unprivileged users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.20	Ensure the operating system has the packages required for multifactor authentication (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.21	Ensure the operating system implements certificate status checking for multifactor authentication (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.22	Ensure the operating system accepts PIV credentials (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.23	Ensure the NX (no-execution) bit flag is set on the system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.24	Ensure kernel page-table isolation is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.25	Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.26	Ensure the operating system restricts usage of ptrace to descendant processes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.27	Ensure the operating system restricts exposed kernel pointer addresses access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.28	Ensure the operating system disables the ability to load the firewire-core kernel module (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.29	Ensure the operating system disables the ability to load the USB Storage kernel module (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.30	Ensure the operating system disables the use of user namespaces (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.31	Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.32	Ensure the "tmux" package installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

1.33	Ensure the operating system enables hardening for the BPF JIT (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.34	Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2	Services		
2.1	inetd Services		
2.1.1	Ensure xinetd is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Special Purpose Services		
2.2.1	Time Synchronization		
2.2.1.1	Ensure time synchronization is in use (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.2	Ensure chrony is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.3	Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.4	Ensure the operating system disables the chrony daemon from acting as a server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.5	Ensure the operating system disables network management of the chrony daemon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure X Window System is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure rsync service is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure Avahi Server is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure SNMP Server is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure HTTP Proxy Server is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Ensure Samba is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Ensure IMAP and POP3 server is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	Ensure HTTP server is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	Ensure FTP Server is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure DNS Server is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.12	Ensure NFS is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure RPC is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	Ensure LDAP server is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	Ensure DHCP Server is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	Ensure the telnet-server package is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.17	Ensure CUPS is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.18	Ensure NIS Server is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.19	Ensure mail transfer agent is configured for local-only mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.20	Ensure the operating system has enabled the hardware random number generator entropy gatherer service (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.21	Ensure automated bug reporting tools are not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.22	Ensure the sendmail package is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.23	Ensure the rsh-server package is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

2.2.24	Ensure a camera is not installed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.25	Ensure the operating system is configured to mask the debug-shell systemd service (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.26	Ensure a TFTP server has not been installed on the system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.27	Ensure the operating system is configured to prevent unrestricted mail relaying (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.28	Ensure the TFTP daemon is configured to operate in secure mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.29	Ensure an FTP server has not been installed on the system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.30	Ensure the gssproxy package has not been installed on the system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.31	Ensure the iputils package has not been installed on the system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.32	Ensure the tuned package has not been installed on the system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.33	Ensure the krb5-server package has not been installed on the system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Service Clients		
2.3.1	Ensure NIS Client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure telnet client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure LDAP client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3	Network Configuration		
3.1	Network Parameters (Host Only)		
3.1.1	Ensure IP forwarding is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure packet redirect sending is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure the system does not accept router advertisements on IPv6 interfaces, unless the system is a router (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure the system does not accept router advertisements on IPv6 interfaces by default, unless the system is a router (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Network Parameters (Host and Router)		
3.2.1	Ensure source routed packets are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure Reverse Path Filtering is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.8	Ensure TCP SYN Cookies is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.9	Ensure IPv6 router advertisements are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

3.2.10	Ensure the operating system does not accept IPv6 ICMP redirect messages (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.11	Ensure the operating system does not accept IPv6 source-routed packets (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.12	Ensure the operating system does not accept IPv6 source-routed packets by default (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.13	Ensure the operating system ignores IPv6 ICMP redirect messages (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.14	Ensure network interfaces are not in promiscuous mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.15	Ensure the operating system does not accept IPv4 ICMP redirect messages (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.16	Ensure the operating system does not accept IPv4 source-routed packet (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.17	Ensure the operating system does not accept IPv4 source-routed packets by default (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.18	Ensure the operating system ignores IPv4 ICMP redirect messages (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Uncommon Network Protocols		
3.3.1	Ensure DCCP is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure SCTP is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure RDS is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure TIPC is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure ATM is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure CAN is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Firewall Configuration		
3.4.1	Ensure Firewall software is installed		
3.4.1.1	Ensure a Firewall package is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2	Configure firewalld		
3.4.2.1	Ensure firewalld service is enabled and running (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure iptables service is not enabled with firewalld (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.3	Ensure nftables is not enabled with firewalld (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.4	Ensure firewalld default zone is set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.5	Ensure network interfaces are assigned to appropriate zone (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.6	Ensure firewalld drops unnecessary services and ports (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.7	Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.8	Ensure "firewalld" is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3	Configure nftables		
3.4.3.1	Ensure iptables are flushed with nftables (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

3.4.3.2	Ensure an nftables table exists (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.3	Ensure nftables base chains exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.4	Ensure nftables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.5	Ensure nftables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.6	Ensure nftables default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.7	Ensure nftables service is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.8	Ensure nftables rules are permanent (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.9	Ensure "nftables" is configured to allow rate limits on any connection to the system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4	Configure iptables		
3.4.4.1	Configure IPv4 iptables		
3.4.4.1.1	Ensure iptables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.2	Ensure iptables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.3	Ensure iptables firewall rules exist for all open ports (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.4	Ensure iptables default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.5	Ensure iptables is enabled and active (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2	Configure IPv6 ip6tables		
3.4.4.2.1	Ensure ip6tables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.2	Ensure ip6tables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.3	Ensure ip6tables firewall rules exist for all open ports (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.4	Ensure ip6tables default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.5	Ensure ip6tables is enabled and active (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Ensure wireless interfaces are disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Disable IPv6 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure at least two name servers are configured if using DNS resolution (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure Bluetooth is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4	Logging and Auditing		
4.1	Configure System Accounting (auditd)		
4.1.1	Ensure auditing is enabled		
4.1.1.1	Ensure auditd is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Ensure auditd service is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	Ensure audit_backlog_limit is sufficient (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.5	Ensure the audit service is configured to produce audit records (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Configure Data Retention		

4.1.2.1	Ensure audit log storage size is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.2	Ensure audit logs are not automatically deleted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.3	Ensure system is disabled when audit logs are full (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.4	Ensure the operating system allocates audit record storage capacity (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.5	Ensure the operating system has the packages required for offloading audit logs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.6	Ensure the operating system has the packages required for encrypting offloaded audit logs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.7	Ensure the audit system off-loads audit records onto a different system or media from the system being audited (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.8	Ensure the audit system is configured to take an appropriate action when the internal event queue is full (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.9	Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.10	Ensure the the operating system authenticates the remote logging server for off-loading audit logs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.11	Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure changes to system administration scope (sudoers) is collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure the SA and ISSO are notified in the event of an audit processing failure (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure the SA and ISSO are notified when the audit storage volume is full (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure an audit event is generated for any successful/unsuccessful use of the "chage" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure the operating system is configured to audit the execution of the "fremovexattr" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.8	Ensure the operating system is configured to audit the execution of the "fsetxattr" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.9	Ensure the operating system is configured to audit the execution of the "lsetxattr" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.10	Ensure the operating system is configured to audit the execution of the "removexattr" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.11	Ensure the operating system is configured to audit the execution of the "lremovexattr" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.12	Ensure the operating system generates audit records when successful/unsuccessful attempts to use the "su" command	<input type="checkbox"/>	<input type="checkbox"/>

	by performing the following command to check the file system rules in "/etc/audit/audit.rules" (Automated)		
4.1.13	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.14	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.15	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.16	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.17	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.18	Ensure the audit system prevents unauthorized changes to logon UIDs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.19	Ensure the audit system prevents unauthorized changes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.20	Ensure the operating system takes the appropriate action when the audit storage volume is full (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.21	Ensure the operating system takes the appropriate action when the audit storage volume is full (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.22	Ensure login and logout events are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.23	Ensure the operating system takes the appropriate action when an audit processing failure occurs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.24	Ensure session initiation information is collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.25	Ensure events that modify date and time information are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.26	Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.27	Ensure events that modify the system's network environment are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.28	Ensure discretionary access control permission modification events are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.29	Ensure unsuccessful unauthorized file access attempts are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.30	Ensure events that modify user/group information are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.31	Ensure successful file system mounts are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.32	Ensure use of privileged commands is collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

4.1.33	Ensure file deletion events by users are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.34	Ensure kernel module loading and unloading is collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.35	Ensure system administrator actions (sudolog) are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.36	Ensure the audit configuration is immutable (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.37	Ensure the operating system audits the execution of privileged functions (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.38	Ensure the operating system's audit daemon is configured to include local events (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.39	Ensure the operating system's audit daemon is configured to label all off-loaded audit logs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.40	Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.41	Ensure the operating system's audit logs have a mode of "0600" or less permissive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.42	Ensure the operating system's audit logs are owned by "root" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.43	Ensure the audit logs are group-owned by "root" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.44	Ensure the audit log directory is owned by "root" to prevent unauthorized read access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.45	Ensure the audit log directory is group-owned by "root" to prevent unauthorized read access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.46	Ensure the audit log directories have a mode of "0700" or less permissive by first determining where the audit logs are stored (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.47	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chcon" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.48	Ensure the operating system is configured to audit the execution of the "setxattr" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.49	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.50	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.51	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-agent" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.52	Ensure an audit event is generated for any successful/unsuccessful use of the "passwd" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

4.1.53	Ensure an audit event is generated for any successful/unsuccessful use of the "mount" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.54	Ensure an audit event is generated for any successful/unsuccessful use of the "umount" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.55	Ensure an audit event is generated for any successful/unsuccessful use of the "mount" syscall (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.56	Ensure an audit event is generated for any successful/unsuccessful use of the "unix_update" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.57	Ensure an audit event is generated for any successful/unsuccessful use of "postdrop" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.58	Ensure an audit event is generated for any successful/unsuccessful use of "postqueue" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.59	Ensure an audit event is generated for any successful/unsuccessful use of "semanage" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.60	Ensure an audit event is generated for any successful/unsuccessful use of "setfiles" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.61	Ensure an audit event is generated for any successful/unsuccessful use of "userhelper" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.62	Ensure an audit event is generated for any successful/unsuccessful use of "setsebool" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.63	Ensure an audit event is generated for any successful/unsuccessful use of "unix_chkpwd" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.64	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-keysign" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.65	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "setfacl" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.66	Ensure an audit event is generated for any successful/unsuccessful use of the "pam_timestamp_check" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.67	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "newgrp" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.68	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "init_module" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.69	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rename" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

4.1.70	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "renameat" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.71	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rmdir" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.72	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlink" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.73	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlinkat" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.74	Ensure an audit event is generated for any successful/unsuccessful use of the "gpasswd" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.75	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "finit_module" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.76	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "delete_module" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.77	Ensure an audit event is generated for any successful/unsuccessful use of the "crontab" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.78	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chsh" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.79	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "truncate" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.80	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "openat" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.81	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.82	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open_by_handle_at" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.83	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ftruncate" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.84	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "creat" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

4.1.85	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chown" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.86	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chmod" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.87	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "lchown" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.88	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchownat" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.89	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchown" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.90	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmod" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.91	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmodat" system call (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.92	Ensure an audit event is generated for any successful/unsuccessful use of the "sudo" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.93	Ensure an audit event is generated for any successful/unsuccessful use of the "usermod" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.94	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chacl" command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.95	Ensure the operating system is configured to audit the execution of the module management program "kmod" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.96	Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "faillock" file occur (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.97	Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "lastlog" file (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.98	Ensure the operating system enables auditing of processes that start prior to the audit daemon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.99	Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.100	Ensure the operating system enables Linux audit logging of the USBGuard daemon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

4.1.101	Ensure the files in directory "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.102	Ensure the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.103	Ensure the audit tools are owned by "root" to prevent any unauthorized access, deletion, or modification (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.104	Ensure the audit tools are group-owned by "root" to prevent any unauthorized access, deletion, or modification (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.105	Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Configure Logging		
4.2.1	Configure rsyslog		
4.2.1.1	Ensure rsyslog is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.2	Ensure the rsyslog service is enabled and active (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.3	Ensure the operating system monitors all remote access methods (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.4	Ensure rsyslog Service is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.5	Ensure rsyslog default file permissions configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.6	Ensure logging is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.7	Ensure rsyslog is configured to send logs to a remote log host (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.8	Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.9	Ensure "rsyslog" is configured to log cron events (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	Configure journald		
4.2.2.1	Ensure journald is configured to send logs to rsyslog (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.2	Ensure journald is configured to compress large log files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure permissions on all logfiles are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure logrotate is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure administrators are notified if an audit processing failure occurs by modifying "/etc/aliases" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5	Access, Authentication and Authorization		
5.1	Configure cron		

5.1.1	Ensure cron daemon is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure permissions on /etc/crontab are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure permissions on /etc/cron.daily are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure permissions on /etc/cron.d are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.8	Ensure at/cron is restricted to authorized users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2	SSH Server Configuration		
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure SSH private key files have a passcode (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure SSH access is limited (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure permissions on SSH private host key files are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure permissions on SSH public host key files are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure SSH LogLevel is appropriate (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure SSH X11 forwarding is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	Ensure SSH MaxAuthTries is set to 4 or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	Ensure SSH IgnoreRhosts is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	Ensure SSH HostbasedAuthentication is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	Ensure SSH root login is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	Ensure SSH PermitEmptyPasswords is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.14	Ensure SSH PermitUserEnvironment is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.15	Ensure SSH Idle Timeout Interval is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.16	Ensure SSH LoginGraceTime is set to one minute or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.17	Ensure SSH warning banner is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.18	Ensure SSH PAM is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.19	Ensure SSH AllowTcpForwarding is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.20	Ensure SSH MaxStartups is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

5.2.21	Ensure SSH MaxSessions is set to 4 or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.22	Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.23	Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.24	Ensure the SSH server uses strong entropy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.25	Ensure system-wide crypto policy is not over-ridden (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.26	Ensure the SSH daemon performs strict mode checking of home directory configuration files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.27	Ensure the SSH daemon performs compression after a user successfully authenticates (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.28	Ensure the SSH daemon does not allow authentication using known host's authentication (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.29	Ensure the SSH daemon does not allow Kerberos authentication (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.30	Ensure null passwords cannot be used (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.31	Ensure SSH provides users with feedback on when account accesses last occurred (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.32	Ensure SSH is loaded and active (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.33	Ensure the SSH server is configured to force frequent session key renegotiation (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.34	Ensure the SSH daemon prevents remote hosts from connecting to the proxy display (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.35	Ensure system-wide crypto policies are in effect (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.36	Ensure the SSH daemon does not allow GSSAPI authentication (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.37	Ensure SSH is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.38	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3	Configure authselect		
5.3.1	Create custom authselect profile (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2	Select authselect profile (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	Ensure authselect includes with-faillock (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4	Configure PAM		
5.4.1	Ensure password creation requirements are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2	Ensure the system locks an account after three unsuccessful logon attempts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3	Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts within 15 minutes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

5.4.4	Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.5	Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.6	Ensure lockout for failed password attempts is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.7	Ensure password reuse is limited (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.8	Ensure password hashing algorithm is SHA-512 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.9	Ensure a minimum number of hash rounds is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.10	Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes until released by an administrator (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.11	Ensure the "/etc/security/faillock.conf" file is configured to lock an account until released by an administrator after three unsuccessful logon attempts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.12	Ensure the faillock directory contents persist after a reboot (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.13	Ensure the "/etc/security/faillock.conf" file is configured to use a non-default faillock directory to ensure contents persist after reboot (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.14	Ensure the system prevents informative messages to the user about logon information (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.15	Ensure the "/etc/security/faillock.conf" file is configured to prevent informative messages about logon attempts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.16	Ensure the system logs user name information when unsuccessful logon attempts occur (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.17	Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.18	Ensure the system includes the root account when locking an account after three unsuccessful logon attempts within a period of 15 minutes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.19	Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.20	Ensure the operating system prohibits password reuse for a minimum of five generations (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.21	Ensure the operating system uses multifactor authentication for local access to accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.22	Ensure the date and time of the last successful account logon upon logon is displayed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

5.4.23	Ensure the "pam_unix.so" module is configured to use sha512 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.24	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/system-auth" file (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.25	Ensure blank or null passwords in the "system-auth" file cannot be used (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.26	Ensure blank or null passwords in the "password-auth" file cannot be used (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.27	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/password-auth" file (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5	User Accounts and Environment		
5.5.1	Set Shadow Password Suite Parameters		
5.5.1.1	Ensure password expiration is 365 days or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.2	Ensure the shadow password suite configuration is set to encrypt password with a FIPS 140-2 approved cryptographic hashing algorithm. (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.3	Ensure the value of the "maxrepeat" option in "/etc/security/pwquality.conf" is "3" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.4	Ensure the value of the "difok" option in "/etc/security/pwquality.conf" is "8" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.5	Ensure the value of the "minclass" option in "/etc/security/pwquality.conf" is "4" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.6	Ensure the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" is "4" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.7	Ensure the value for "dcredit" in "/etc/security/pwquality.conf" is "-1" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.8	Ensure the value for "lcredit" in "/etc/security/pwquality.conf" is "-1" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.9	Ensure the value for "ucredit" in "/etc/security/pwquality.conf" is "-1" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.10	Ensure the operating system uses "pwquality" to enforce the password complexity rules (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.11	Ensure minimum days between password changes is 7 or more (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.12	Ensure password expiration warning days is 7 or more (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.13	Ensure inactive password lock is 30 days or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.14	Ensure all users last password change date is in the past (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.15	Ensure the minimum time period between password changes for each user account is one day or greater (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

5.5.1.16	Ensure the operating system enforces 24 hours/1 day as the minimum password lifetime for new user accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.17	Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.18	Ensure the maximum time period for existing passwords is restricted to 60 days (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.19	Ensure the operating system enforces a minimum 15-character password length (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.20	Ensure the operating system enforces a minimum 15-character password length for new user accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.21	Ensure the value for "ocredit" in "/etc/security/pwquality.conf" is "-1" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.22	Ensure the operating system prevents the use of dictionary words for passwords (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.23	Ensure the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.2	Ensure system accounts are secured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.3	Ensure default user shell timeout is 900 seconds or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.4	Ensure the interactive user account passwords are using a strong password hash (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.5	Ensure default group for the root account is GID 0 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.6	Ensure default user umask is 027 or more restrictive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.7	Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.9	Ensure the default umask for all local interactive users is "077" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.10	Ensure the umask default for installed shells is "077" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.11	Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.6	Ensure root login is restricted to system console (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure PKI-based authentication has valid certificates (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.8	Ensure access to the su command is restricted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.9	Ensure the operating system prevents system daemons from using Kerberos for authentication (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

5.10	Ensure the krb5-workstation package has not been installed on the system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.11	Ensure SSSD prohibits the use of cached authentications after one day (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.12	Ensure "fapolicyd" is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.13	Ensure USBGuard has a policy configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.14	Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.15	Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.16	Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.17	Ensure "fapolicyd" is enabled and running (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.18	Ensure "fapolicyd" employs a deny-all, permit-by-exception policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.19	Ensure USBGuard is installed on the operating system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.20	Ensure the operating system has enabled the use of the USBGuard (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6	System Maintenance		
6.1	System File Permissions		
6.1.1	Audit system file permissions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure permissions on /etc/passwd are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Ensure permissions on /etc/passwd- are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.4	Ensure permissions on /etc/shadow are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.5	Ensure permissions on /etc/shadow- are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.6	Ensure permissions on /etc/gshadow are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.7	Ensure permissions on /etc/gshadow- are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.8	Ensure permissions on /etc/group are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.9	Ensure permissions on /etc/group- are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.10	Ensure the root account is the only account that has unrestricted access to the operating system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.11	Ensure no world writable files exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.12	Ensure no unowned files or directories exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.13	Ensure no ungrouped files or directories exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.14	Ensure all public directories are owned by root or a system account (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

6.1.15	Audit SUID executables (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.16	Audit SGID executables (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.17	Ensure the "/var/log/messages" file has mode "0640" or less permissive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.18	Ensure the "/var/log/messages" file is owned by root (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.19	Ensure the "/var/log/messages" file is group-owned by root (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.20	Ensure the "/var/log" directory has a mode of "0755" or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.21	Ensure the "/var/log" directory is owned by root (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.22	Ensure the "/var/log" directory is group-owned by root (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.23	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories have mode "0755" or less permissive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.24	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are owned by "root" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.25	Ensure the system commands contained in "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are group-owned by "root" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.26	Ensure the system-wide shared library files contained in the "/lib, /lib64, /usr/lib, /usr/lib64" directories have mode "0755" or less permissive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.27	Ensure the system-wide shared library files are owned by "root" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.28	Ensure the system-wide shared library files are group-owned by "root" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.29	Ensure world-writable directories are owned by root, sys, bin, or an application user (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.30	Ensure world-writable directories are group-owned by root, sys, bin, or an application group (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.31	Ensure local initialization files do not execute world-writable programs (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.32	Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.33	Ensure the operating system prevents users from disabling the tmux terminal multiplexer (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.34	Ensure the operating system enables a user's session lock until that user re-establishes access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

6.1.35	Ensure the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.36	Ensure the operating system initiates a session lock after 15 minutes of inactivity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.37	Ensure all accounts on the system are assigned to an active system, application, or user account (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.2	User and Group Settings		
6.2.1	Ensure password fields are not empty (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Ensure root PATH Integrity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Ensure no legacy "+" entries exist in /etc/shadow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure no legacy "+" entries exist in /etc/group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure root is the only UID 0 account (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure users' home directories permissions are 750 or more restrictive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.9	Ensure users own their home directories (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.10	Ensure users' dot files are not group or world writable (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.11	Ensure no users have .forward files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.12	Ensure no users have .netrc files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.13	Ensure users' .netrc Files are not group or world accessible (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.14	Ensure no users have .rhosts files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.15	Ensure all groups in /etc/passwd exist in /etc/group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.16	Ensure no duplicate UIDs exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.17	Ensure no duplicate GIDs exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.18	Ensure no duplicate user names exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.19	Ensure no duplicate group names exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.20	Ensure shadow group is empty (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.21	Ensure all users' home directories exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.22	Ensure the assigned home directory of all local interactive users is group-owned by that user's primary GID (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.23	Ensure the assigned home directory of all local interactive users exists (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.24	Ensure all local interactive users are assigned a home directory upon creation (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

6.2.25	Ensure all local initialization files have a mode of "0740" or less permissive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.26	Ensure all local files and directories have a valid owner (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.27	Ensure all local files and directories have a valid group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.28	Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.29	Ensure file executable search path statements do not share sensitive home directory information (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.30	Ensure local interactive users have a home directory assigned (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.31	Ensure the operating system limits the number of concurrent sessions to "10" for all accounts and/or account types (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.32	Ensure the operating system enables a user's session lock until that user re-establishes access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.33	Ensure the operating system enables the user to initiate a session lock (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.34	Ensure the operating system prevents a user from overriding settings for graphical user interfaces (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.35	Ensure all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.36	Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.37	Ensure temporary accounts have been provisioned with an expiration date of 72 hours (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure the operating system removes all software components after updated versions have been installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure there are no ".shosts" files on the operating system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Ensure there are no "shosts.equiv" files on the operating system (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of cramfs filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure mounting of vFAT filesystems is limited	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure mounting of squashfs filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure mounting of udf filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Ensure nodev option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Ensure nosuid option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Ensure noexec option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	Ensure separate partition exists for /var	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Ensure separate partition exists for /var/tmp	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Ensure nodev option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Ensure nosuid option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Ensure noexec option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.13	Ensure separate partition exists for /home	<input type="checkbox"/>	<input type="checkbox"/>
1.1.14	Ensure nodev option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.15	Ensure nodev option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.16	Ensure nosuid option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.17	Ensure noexec option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.18	Ensure nodev option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.19	Ensure nosuid option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.20	Ensure noexec option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.21	Ensure sticky bit is set on all world-writable directories	<input type="checkbox"/>	<input type="checkbox"/>
1.1.22	Disable Automounting	<input type="checkbox"/>	<input type="checkbox"/>
1.1.23	Disable USB Storage	<input type="checkbox"/>	<input type="checkbox"/>
1.1.24	Ensure file systems that contain user home directories are mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.25	Ensure the "/boot" directory is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.26	Ensure all non-root local partitions are mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.27	Ensure file systems that are being NFS-imported are mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.29	Ensure file systems being imported via NFS are mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.30	Ensure a separate file system/partition has been created for non-privileged local interactive user home directories	<input type="checkbox"/>	<input type="checkbox"/>
1.1.37	Ensure the "/boot/efi" directory is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>

1.1.38	Ensure file systems that contain user home directories are mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1	Ensure GPG keys are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Ensure gpgcheck is globally activated	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Ensure package manager repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Ensure DNF is configured to perform a signature check on local packages	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Ensure sudo is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Ensure the "/etc/sudoers" file has no occurrences of "NOPASSWD"	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	Ensure the "/etc/sudoers" file has no occurrences of "!authenticate"	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure permissions on bootloader config are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure bootloader password is set	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Ensure authentication required for single user mode	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Ensure the encrypted grub superusers password is set for systems booted with UEFI	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Ensure the encrypted grub superusers password is set for system booted with BIOS	<input type="checkbox"/>	<input type="checkbox"/>
1.5.6	Ensure the operating system requires authentication for rescue mode	<input type="checkbox"/>	<input type="checkbox"/>
1.5.7	Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities	<input type="checkbox"/>	<input type="checkbox"/>
1.5.8	Ensure GRUB 2 is configured to disable vsyscalls	<input type="checkbox"/>	<input type="checkbox"/>
1.5.9	Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities	<input type="checkbox"/>	<input type="checkbox"/>
1.5.10	Ensure the operating system is configured to boot to the command line	<input type="checkbox"/>	<input type="checkbox"/>
1.5.11	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed	<input type="checkbox"/>	<input type="checkbox"/>
1.5.12	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds	<input type="checkbox"/>	<input type="checkbox"/>
1.5.13	Ensure a unique name is set as the "superusers" account (UEFI)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.14	Ensure a unique name is set as the "superusers" account (BIOS)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.15	Ensure the operating system requires authentication upon booting into emergency mode	<input type="checkbox"/>	<input type="checkbox"/>
1.6.1	Ensure core dumps are restricted	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure the operating system is not configured to acquire, save, or process core dumps	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure kernel core dumps are disabled unless needed	<input type="checkbox"/>	<input type="checkbox"/>

1.6.6	Ensure the operating system disables core dumps for all users	<input type="checkbox"/>	<input type="checkbox"/>
1.6.7	Ensure the operating system disables storing core dumps for all users	<input type="checkbox"/>	<input type="checkbox"/>
1.6.8	Ensure the operating system disables core dump backtraces	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.1	Ensure SELinux is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.2	Ensure SELinux is not disabled in bootloader configuration	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.3	Ensure SELinux policy is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.4	Ensure the SELinux state is enforcing	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.6	Ensure SETroubleshoot is not installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.8	Ensure the operating system has the policycoreutils package installed	<input type="checkbox"/>	<input type="checkbox"/>
1.8.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.8.2	Ensure message of the day is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.3	Ensure local login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.4	Ensure remote login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.5	Ensure permissions on /etc/motd are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.6	Ensure permissions on /etc/issue are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.7	Ensure permissions on /etc/issue.net are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.8	Ensure the Standard Mandatory DoD Notice and Consent Banner is displayed before granting access to the system via SSH logon	<input type="checkbox"/>	<input type="checkbox"/>
1.8.9	Ensure the operating system displays a banner before granting access to the operating system via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.2	Ensure GNOME Display Manager is removed	<input type="checkbox"/>	<input type="checkbox"/>
1.9.3	Ensure GDM login banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.9.4	Ensure last logged in user display is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.9.6	Ensure a Standard Mandatory DoD Notice and Consent Banner is displayed via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.7	Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.8	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.9	Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated	<input type="checkbox"/>	<input type="checkbox"/>

1.9.10	Ensure the operating system disables the user logon list for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
1.9.11	Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.12	Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.10	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
1.15	Ensure kernel image loading is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure the operating system is configured to enable DAC on symlinks	<input type="checkbox"/>	<input type="checkbox"/>
1.17	Ensure the operating system is configured to enable DAC on hardlinks	<input type="checkbox"/>	<input type="checkbox"/>
1.18	Ensure the operating system is configured to restrict access to the kernel message buffer	<input type="checkbox"/>	<input type="checkbox"/>
1.19	Ensure the operating system is configured to prevent kernel profiling by unprivileged users	<input type="checkbox"/>	<input type="checkbox"/>
1.20	Ensure the operating system has the packages required for multifactor authentication	<input type="checkbox"/>	<input type="checkbox"/>
1.22	Ensure the operating system accepts PIV credentials	<input type="checkbox"/>	<input type="checkbox"/>
1.24	Ensure kernel page-table isolation is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.25	Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall	<input type="checkbox"/>	<input type="checkbox"/>
1.26	Ensure the operating system restricts usage of ptrace to descendant processes	<input type="checkbox"/>	<input type="checkbox"/>
1.27	Ensure the operating system restricts exposed kernel pointer addresses access	<input type="checkbox"/>	<input type="checkbox"/>
1.30	Ensure the operating system disables the use of user namespaces	<input type="checkbox"/>	<input type="checkbox"/>
1.31	Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service	<input type="checkbox"/>	<input type="checkbox"/>
1.32	Ensure the "tmux" package installed	<input type="checkbox"/>	<input type="checkbox"/>
1.33	Ensure the operating system enables hardening for the BPF JIT	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure X Window System is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.20	Ensure the operating system has enabled the hardware random number generator entropy gatherer service	<input type="checkbox"/>	<input type="checkbox"/>
2.2.28	Ensure the TFTP daemon is configured to operate in secure mode	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure NIS Client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure LDAP client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure IP forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>

3.1.3	Ensure the system does not accept router advertisements on IPv6 interfaces, unless the system is a router	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure the system does not accept router advertisements on IPv6 interfaces by default, unless the system is a router	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure Reverse Path Filtering is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.8	Ensure TCP SYN Cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.9	Ensure IPv6 router advertisements are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.10	Ensure the operating system does not accept IPv6 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.11	Ensure the operating system does not accept IPv6 source-routed packets	<input type="checkbox"/>	<input type="checkbox"/>
3.2.12	Ensure the operating system does not accept IPv6 source-routed packets by default	<input type="checkbox"/>	<input type="checkbox"/>
3.2.13	Ensure the operating system ignores IPv6 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.14	Ensure network interfaces are not in promiscuous mode	<input type="checkbox"/>	<input type="checkbox"/>
3.2.15	Ensure the operating system does not accept IPv4 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.16	Ensure the operating system does not accept IPv4 source-routed packet	<input type="checkbox"/>	<input type="checkbox"/>
3.2.17	Ensure the operating system does not accept IPv4 source-routed packets by default	<input type="checkbox"/>	<input type="checkbox"/>
3.2.18	Ensure the operating system ignores IPv4 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.1	Ensure a Firewall package is installed	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.1	Ensure firewalld service is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure iptables service is not enabled with firewalld	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.3	Ensure nftables is not enabled with firewalld	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.4	Ensure firewalld default zone is set	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.5	Ensure network interfaces are assigned to appropriate zone	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.6	Ensure firewalld drops unnecessary services and ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.7	Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.8	Ensure "firewalld" is installed	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.1	Ensure iptables are flushed with nftables	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.2	Ensure an nftables table exists	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.3	Ensure nftables base chains exist	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.4	Ensure nftables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>

3.4.3.5	Ensure nftables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.6	Ensure nftables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.7	Ensure nftables service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.8	Ensure nftables rules are permanent	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.9	Ensure "nftables" is configured to allow rate limits on any connection to the system	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.1	Ensure iptables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.2	Ensure iptables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.3	Ensure iptables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.4	Ensure iptables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.5	Ensure iptables is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.1	Ensure ip6tables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.2	Ensure ip6tables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.3	Ensure ip6tables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.4	Ensure ip6tables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.5	Ensure ip6tables is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure at least two name servers are configured if using DNS resolution	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Ensure auditd is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Ensure auditd service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	Ensure audit_backlog_limit is sufficient	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.5	Ensure the audit service is configured to produce audit records	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure the SA and ISSO are notified in the event of an audit processing failure	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure an audit event is generated for any successful/unsuccessful use of the "chage" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure the operating system is configured to audit the execution of the "fremovexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.8	Ensure the operating system is configured to audit the execution of the "fsetxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.9	Ensure the operating system is configured to audit the execution of the "lsetxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.10	Ensure the operating system is configured to audit the execution of the "removexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.11	Ensure the operating system is configured to audit the execution of the "lremovexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>

4.1.16	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.17	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.18	Ensure the audit system prevents unauthorized changes to logon UIDs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.19	Ensure the audit system prevents unauthorized changes	<input type="checkbox"/>	<input type="checkbox"/>
4.1.23	Ensure the operating system takes the appropriate action when an audit processing failure occurs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.31	Ensure successful file system mounts are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.32	Ensure use of privileged commands is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.34	Ensure kernel module loading and unloading is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.36	Ensure the audit configuration is immutable	<input type="checkbox"/>	<input type="checkbox"/>
4.1.37	Ensure the operating system audits the execution of privileged functions	<input type="checkbox"/>	<input type="checkbox"/>
4.1.38	Ensure the operating system's audit daemon is configured to include local events	<input type="checkbox"/>	<input type="checkbox"/>
4.1.40	Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.41	Ensure the operating system's audit logs have a mode of "0600" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
4.1.42	Ensure the operating system's audit logs are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.43	Ensure the audit logs are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.44	Ensure the audit log directory is owned by "root" to prevent unauthorized read access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.45	Ensure the audit log directory is group-owned by "root" to prevent unauthorized read access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.46	Ensure the audit log directories have a mode of "0700" or less permissive by first determining where the audit logs are stored	<input type="checkbox"/>	<input type="checkbox"/>
4.1.47	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chcon" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.48	Ensure the operating system is configured to audit the execution of the "setxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.49	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.50	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group"	<input type="checkbox"/>	<input type="checkbox"/>

4.1.51	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-agent"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.52	Ensure an audit event is generated for any successful/unsuccessful use of the "passwd" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.53	Ensure an audit event is generated for any successful/unsuccessful use of the "mount" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.54	Ensure an audit event is generated for any successful/unsuccessful use of the "umount" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.55	Ensure an audit event is generated for any successful/unsuccessful use of the "mount" syscall	<input type="checkbox"/>	<input type="checkbox"/>
4.1.56	Ensure an audit event is generated for any successful/unsuccessful use of the "unix_update"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.57	Ensure an audit event is generated for any successful/unsuccessful use of "postdrop"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.58	Ensure an audit event is generated for any successful/unsuccessful use of "postqueue"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.59	Ensure an audit event is generated for any successful/unsuccessful use of "semanage"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.60	Ensure an audit event is generated for any successful/unsuccessful use of "setfiles"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.61	Ensure an audit event is generated for any successful/unsuccessful use of "userhelper"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.62	Ensure an audit event is generated for any successful/unsuccessful use of "setsebool"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.63	Ensure an audit event is generated for any successful/unsuccessful use of "unix_chkpwd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.64	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-keysign"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.65	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "setfacl" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.66	Ensure an audit event is generated for any successful/unsuccessful use of the "pam_timestamp_check" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.67	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "newgrp" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.68	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "init_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.69	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rename" command	<input type="checkbox"/>	<input type="checkbox"/>

4.1.70	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "renameat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.71	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rmdir" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.72	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlink" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.73	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlinkat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.74	Ensure an audit event is generated for any successful/unsuccessful use of the "gpasswd" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.75	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "finit_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.76	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "delete_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.77	Ensure an audit event is generated for any successful/unsuccessful use of the "crontab" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.78	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chsh" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.79	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "truncate" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.80	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "openat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.81	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.82	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open_by_handle_at" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.83	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ftruncate" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.84	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "creat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.85	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chown" command	<input type="checkbox"/>	<input type="checkbox"/>

4.1.86	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chmod" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.87	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "lchown" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.88	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchownat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.89	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchown" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.90	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmod" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.91	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmodat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.93	Ensure an audit event is generated for any successful/unsuccessful use of the "usermod" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.94	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chacl" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.95	Ensure the operating system is configured to audit the execution of the module management program "kmod"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.96	Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "faillock" file occur	<input type="checkbox"/>	<input type="checkbox"/>
4.1.97	Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "lastlog" file	<input type="checkbox"/>	<input type="checkbox"/>
4.1.98	Ensure the operating system enables auditing of processes that start prior to the audit daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.99	Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.100	Ensure the operating system enables Linux audit logging of the USBGuard daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.101	Ensure the files in directory "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
4.1.102	Ensure the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode	<input type="checkbox"/>	<input type="checkbox"/>
4.1.103	Ensure the audit tools are owned by "root" to prevent any unauthorized access, deletion, or modification	<input type="checkbox"/>	<input type="checkbox"/>

4.1.104	Ensure the audit tools are group-owned by "root" to prevent any unauthorized access, deletion, or modification	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.1	Ensure rsyslog is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.3	Ensure the operating system monitors all remote access methods	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.4	Ensure rsyslog Service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.5	Ensure rsyslog default file permissions configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.6	Ensure logging is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure permissions on all logfiles are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure administrators are notified if an audit processing failure occurs by modifying "/etc/aliases"	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure cron daemon is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure permissions on /etc/crontab are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on /etc/cron.hourly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure permissions on /etc/cron.daily are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure permissions on /etc/cron.weekly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure permissions on /etc/cron.monthly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure permissions on /etc/cron.d are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure SSH private key files have a passcode	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure SSH access is limited	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure permissions on SSH private host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure permissions on SSH public host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure SSH LogLevel is appropriate	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	Ensure SSH root login is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.2.14	Ensure SSH PermitUserEnvironment is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.15	Ensure SSH Idle Timeout Interval is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.16	Ensure SSH LoginGraceTime is set to one minute or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.17	Ensure SSH warning banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.18	Ensure SSH PAM is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.20	Ensure SSH MaxStartups is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.21	Ensure SSH MaxSessions is set to 4 or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.24	Ensure the SSH server uses strong entropy	<input type="checkbox"/>	<input type="checkbox"/>
5.2.26	Ensure the SSH daemon performs strict mode checking of home directory configuration files	<input type="checkbox"/>	<input type="checkbox"/>
5.2.27	Ensure the SSH daemon performs compression after a user successfully authenticates	<input type="checkbox"/>	<input type="checkbox"/>

5.2.28	Ensure the SSH daemon does not allow authentication using known host's authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.29	Ensure the SSH daemon does not allow Kerberos authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.31	Ensure SSH provides users with feedback on when account accesses last occurred	<input type="checkbox"/>	<input type="checkbox"/>
5.2.33	Ensure the SSH server is configured to force frequent session key renegotiation	<input type="checkbox"/>	<input type="checkbox"/>
5.2.34	Ensure the SSH daemon prevents remote hosts from connecting to the proxy display	<input type="checkbox"/>	<input type="checkbox"/>
5.2.36	Ensure the SSH daemon does not allow GSSAPI authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.38	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	Create custom authselect profile	<input type="checkbox"/>	<input type="checkbox"/>
5.4.9	Ensure a minimum number of hash rounds is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.12	Ensure the faillock directory contents persist after a reboot	<input type="checkbox"/>	<input type="checkbox"/>
5.4.13	Ensure the "/etc/security/faillock.conf" file is configured to use a non-default faillock directory to ensure contents persist after reboot	<input type="checkbox"/>	<input type="checkbox"/>
5.4.14	Ensure the system prevents informative messages to the user about logon information	<input type="checkbox"/>	<input type="checkbox"/>
5.4.15	Ensure the "/etc/security/faillock.conf" file is configured to prevent informative messages about logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.22	Ensure the date and time of the last successful account logon upon logon is displayed	<input type="checkbox"/>	<input type="checkbox"/>
5.4.24	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/system-auth" file	<input type="checkbox"/>	<input type="checkbox"/>
5.4.27	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/password-auth" file	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.23	Ensure the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt	<input type="checkbox"/>	<input type="checkbox"/>
5.5.3	Ensure default user shell timeout is 900 seconds or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.5	Ensure default group for the root account is GID 0	<input type="checkbox"/>	<input type="checkbox"/>
5.5.6	Ensure default user umask is 027 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
5.5.7	Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.5.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
5.5.9	Ensure the default umask for all local interactive users is "077"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.10	Ensure the umask default for installed shells is "077"	<input type="checkbox"/>	<input type="checkbox"/>

5.5.11	Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files	<input type="checkbox"/>	<input type="checkbox"/>
5.6	Ensure root login is restricted to system console	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure PKI-based authentication has valid certificates	<input type="checkbox"/>	<input type="checkbox"/>
5.8	Ensure access to the su command is restricted	<input type="checkbox"/>	<input type="checkbox"/>
5.9	Ensure the operating system prevents system daemons from using Kerberos for authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.11	Ensure SSSD prohibits the use of cached authentications after one day	<input type="checkbox"/>	<input type="checkbox"/>
5.12	Ensure "fapolicyd" is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.17	Ensure "fapolicyd" is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
5.18	Ensure "fapolicyd" employs a deny-all, permit-by-exception policy	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Audit system file permissions	<input type="checkbox"/>	<input type="checkbox"/>
6.1.10	Ensure the root account is the only account that has unrestricted access to the operating system	<input type="checkbox"/>	<input type="checkbox"/>
6.1.11	Ensure no world writable files exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.12	Ensure no unowned files or directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.13	Ensure no ungrouped files or directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.14	Ensure all public directories are owned by root or a system account	<input type="checkbox"/>	<input type="checkbox"/>
6.1.15	Audit SUID executables	<input type="checkbox"/>	<input type="checkbox"/>
6.1.16	Audit SGID executables	<input type="checkbox"/>	<input type="checkbox"/>
6.1.17	Ensure the "/var/log/messages" file has mode "0640" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.18	Ensure the "/var/log/messages" file is owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.19	Ensure the "/var/log/messages" file is group-owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.20	Ensure the "/var/log" directory has a mode of "0755" or less	<input type="checkbox"/>	<input type="checkbox"/>
6.1.21	Ensure the "/var/log" directory is owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.22	Ensure the "/var/log" directory is group-owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.23	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories have mode "0755" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.24	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.25	Ensure the system commands contained in "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.26	Ensure the system-wide shared library files contained in the "/lib, /lib64, /usr/lib, /usr/lib64" directories have mode "0755" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.27	Ensure the system-wide shared library files are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>

6.1.28	Ensure the system-wide shared library files are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.29	Ensure world-writable directories are owned by root, sys, bin, or an application user	<input type="checkbox"/>	<input type="checkbox"/>
6.1.30	Ensure world-writable directories are group-owned by root, sys, bin, or an application group	<input type="checkbox"/>	<input type="checkbox"/>
6.1.31	Ensure local initialization files do not execute world-writable programs	<input type="checkbox"/>	<input type="checkbox"/>
6.1.32	Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer	<input type="checkbox"/>	<input type="checkbox"/>
6.1.33	Ensure the operating system prevents users from disabling the tmux terminal multiplexer	<input type="checkbox"/>	<input type="checkbox"/>
6.1.34	Ensure the operating system enables a user's session lock until that user re-establishes access	<input type="checkbox"/>	<input type="checkbox"/>
6.1.35	Ensure the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
6.1.36	Ensure the operating system initiates a session lock after 15 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Ensure root PATH Integrity	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure root is the only UID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure users' home directories permissions are 750 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
6.2.9	Ensure users own their home directories	<input type="checkbox"/>	<input type="checkbox"/>
6.2.10	Ensure users' dot files are not group or world writable	<input type="checkbox"/>	<input type="checkbox"/>
6.2.11	Ensure no users have .forward files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.13	Ensure users' .netrc Files are not group or world accessible	<input type="checkbox"/>	<input type="checkbox"/>
6.2.20	Ensure shadow group is empty	<input type="checkbox"/>	<input type="checkbox"/>
6.2.21	Ensure all users' home directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.22	Ensure the assigned home directory of all local interactive users is group-owned by that user's primary GID	<input type="checkbox"/>	<input type="checkbox"/>
6.2.23	Ensure the assigned home directory of all local interactive users exists	<input type="checkbox"/>	<input type="checkbox"/>
6.2.24	Ensure all local interactive users are assigned a home directory upon creation	<input type="checkbox"/>	<input type="checkbox"/>
6.2.25	Ensure all local initialization files have a mode of "0740" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.2.26	Ensure all local files and directories have a valid owner	<input type="checkbox"/>	<input type="checkbox"/>
6.2.27	Ensure all local files and directories have a valid group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.28	Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file	<input type="checkbox"/>	<input type="checkbox"/>
6.2.29	Ensure file executable search path statements do not share sensitive home directory information	<input type="checkbox"/>	<input type="checkbox"/>

6.2.30	Ensure local interactive users have a home directory assigned	<input type="checkbox"/>	<input type="checkbox"/>
6.2.31	Ensure the operating system limits the number of concurrent sessions to "10" for all accounts and/or account types	<input type="checkbox"/>	<input type="checkbox"/>
6.2.32	Ensure the operating system enables a user's session lock until that user re-establishes access	<input type="checkbox"/>	<input type="checkbox"/>
6.2.33	Ensure the operating system enables the user to initiate a session lock	<input type="checkbox"/>	<input type="checkbox"/>
6.2.34	Ensure the operating system prevents a user from overriding settings for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
6.2.35	Ensure all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750"	<input type="checkbox"/>	<input type="checkbox"/>
6.2.36	Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of	<input type="checkbox"/>	<input type="checkbox"/>
6.2.37	Ensure temporary accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure the operating system removes all software components after updated versions have been installed	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of cramfs filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure mounting of vFAT filesystems is limited	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure mounting of squashfs filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure mounting of udf filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Ensure /tmp is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Ensure nodev option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Ensure nosuid option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Ensure noexec option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	Ensure separate partition exists for /var	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Ensure separate partition exists for /var/tmp	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Ensure nodev option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Ensure nosuid option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Ensure noexec option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.11	Ensure separate partition exists for /var/log	<input type="checkbox"/>	<input type="checkbox"/>
1.1.12	Ensure separate partition exists for /var/log/audit	<input type="checkbox"/>	<input type="checkbox"/>
1.1.13	Ensure separate partition exists for /home	<input type="checkbox"/>	<input type="checkbox"/>
1.1.14	Ensure nodev option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.15	Ensure nodev option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.16	Ensure nosuid option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.17	Ensure noexec option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.18	Ensure nodev option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.19	Ensure nosuid option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.20	Ensure noexec option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.21	Ensure sticky bit is set on all world-writable directories	<input type="checkbox"/>	<input type="checkbox"/>
1.1.22	Disable Automounting	<input type="checkbox"/>	<input type="checkbox"/>
1.1.23	Disable USB Storage	<input type="checkbox"/>	<input type="checkbox"/>
1.1.24	Ensure file systems that contain user home directories are mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.25	Ensure the "/boot" directory is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.26	Ensure all non-root local partitions are mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.27	Ensure file systems that are being NFS-imported are mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.29	Ensure file systems being imported via NFS are mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>

1.1.30	Ensure a separate file system/partition has been created for non-privileged local interactive user home directories	<input type="checkbox"/>	<input type="checkbox"/>
1.1.31	Ensure "/var/log" is mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.32	Ensure "/var/log" is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.33	Ensure "/var/log" is mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.34	Ensure "/var/log/audit" is mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.35	Ensure "/var/log/audit" is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.36	Ensure "/var/log/audit" is mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.37	Ensure the "/boot/efi" directory is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.38	Ensure file systems that contain user home directories are mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1	Ensure GPG keys are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Ensure gpgcheck is globally activated	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Ensure package manager repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Ensure DNF is configured to perform a signature check on local packages	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Ensure sudo is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
1.3.3	Ensure sudo log file exists	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Ensure the "/etc/sudoers" file has no occurrences of "NOPASSWD"	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	Ensure the "/etc/sudoers" file has no occurrences of "!authenticate"	<input type="checkbox"/>	<input type="checkbox"/>
1.3.6	Ensure the "sudoers" file restricts sudo access to authorized personnel	<input type="checkbox"/>	<input type="checkbox"/>
1.3.7	Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation	<input type="checkbox"/>	<input type="checkbox"/>
1.3.8	Ensure the operating system requires re-authentication when using the "sudo" command to elevate privileges	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure permissions on bootloader config are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure bootloader password is set	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Ensure authentication required for single user mode	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Ensure the encrypted grub superusers password is set for systems booted with UEFI	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Ensure the encrypted grub superusers password is set for system booted with BIOS	<input type="checkbox"/>	<input type="checkbox"/>
1.5.6	Ensure the operating system requires authentication for rescue mode	<input type="checkbox"/>	<input type="checkbox"/>
1.5.7	Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities	<input type="checkbox"/>	<input type="checkbox"/>
1.5.8	Ensure GRUB 2 is configured to disable vsyscalls	<input type="checkbox"/>	<input type="checkbox"/>

1.5.9	Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities	<input type="checkbox"/>	<input type="checkbox"/>
1.5.10	Ensure the operating system is configured to boot to the command line	<input type="checkbox"/>	<input type="checkbox"/>
1.5.11	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed	<input type="checkbox"/>	<input type="checkbox"/>
1.5.12	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds	<input type="checkbox"/>	<input type="checkbox"/>
1.5.13	Ensure a unique name is set as the "superusers" account (UEFI)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.14	Ensure a unique name is set as the "superusers" account (BIOS)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.15	Ensure the operating system requires authentication upon booting into emergency mode	<input type="checkbox"/>	<input type="checkbox"/>
1.6.1	Ensure core dumps are restricted	<input type="checkbox"/>	<input type="checkbox"/>
1.6.2	Ensure address space layout randomization (ASLR) is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure the operating system is not configured to acquire, save, or process core dumps	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure kernel core dumps are disabled unless needed	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure the operating system disables core dumps for all users	<input type="checkbox"/>	<input type="checkbox"/>
1.6.7	Ensure the operating system disables storing core dumps for all users	<input type="checkbox"/>	<input type="checkbox"/>
1.6.8	Ensure the operating system disables core dump backtraces	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.1	Ensure SELinux is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.2	Ensure SELinux is not disabled in bootloader configuration	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.3	Ensure SELinux policy is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.4	Ensure the SELinux state is enforcing	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.5	Ensure no unconfined services exist	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.6	Ensure SETroubleshoot is not installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.7	Ensure the MCS Translation Service (mcstrans) is not installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.8	Ensure the operating system has the policycoreutils package installed	<input type="checkbox"/>	<input type="checkbox"/>
1.8.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.8.2	Ensure message of the day is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.3	Ensure local login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.4	Ensure remote login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.5	Ensure permissions on /etc/motd are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.6	Ensure permissions on /etc/issue are configured	<input type="checkbox"/>	<input type="checkbox"/>

1.8.7	Ensure permissions on /etc/issue.net are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.8	Ensure the Standard Mandatory DoD Notice and Consent Banner is displayed before granting access to the system via SSH logon	<input type="checkbox"/>	<input type="checkbox"/>
1.8.9	Ensure the operating system displays a banner before granting access to the operating system via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.2	Ensure GNOME Display Manager is removed	<input type="checkbox"/>	<input type="checkbox"/>
1.9.3	Ensure GDM login banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.9.4	Ensure last logged in user display is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.9.5	Ensure XDCMP is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.9.6	Ensure a Standard Mandatory DoD Notice and Consent Banner is displayed via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.7	Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.8	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.9	Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated	<input type="checkbox"/>	<input type="checkbox"/>
1.9.10	Ensure the operating system disables the user logon list for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
1.9.11	Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.12	Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.10	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure system-wide crypto policy is not legacy	<input type="checkbox"/>	<input type="checkbox"/>
1.12	Ensure system-wide crypto policy is FUTURE or FIPS	<input type="checkbox"/>	<input type="checkbox"/>
1.15	Ensure kernel image loading is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure the operating system is configured to enable DAC on symlinks	<input type="checkbox"/>	<input type="checkbox"/>
1.17	Ensure the operating system is configured to enable DAC on hardlinks	<input type="checkbox"/>	<input type="checkbox"/>
1.18	Ensure the operating system is configured to restrict access to the kernel message buffer	<input type="checkbox"/>	<input type="checkbox"/>
1.19	Ensure the operating system is configured to prevent kernel profiling by unprivileged users	<input type="checkbox"/>	<input type="checkbox"/>

1.20	Ensure the operating system has the packages required for multifactor authentication	<input type="checkbox"/>	<input type="checkbox"/>
1.22	Ensure the operating system accepts PIV credentials	<input type="checkbox"/>	<input type="checkbox"/>
1.23	Ensure the NX (no-execution) bit flag is set on the system	<input type="checkbox"/>	<input type="checkbox"/>
1.24	Ensure kernel page-table isolation is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.25	Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall	<input type="checkbox"/>	<input type="checkbox"/>
1.26	Ensure the operating system restricts usage of ptrace to descendant processes	<input type="checkbox"/>	<input type="checkbox"/>
1.27	Ensure the operating system restricts exposed kernel pointer addresses access	<input type="checkbox"/>	<input type="checkbox"/>
1.28	Ensure the operating system disables the ability to load the firewire-core kernel module	<input type="checkbox"/>	<input type="checkbox"/>
1.29	Ensure the operating system disables the ability to load the USB Storage kernel module	<input type="checkbox"/>	<input type="checkbox"/>
1.30	Ensure the operating system disables the use of user namespaces	<input type="checkbox"/>	<input type="checkbox"/>
1.31	Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service	<input type="checkbox"/>	<input type="checkbox"/>
1.32	Ensure the "tmux" package installed	<input type="checkbox"/>	<input type="checkbox"/>
1.33	Ensure the operating system enables hardening for the BPF JIT	<input type="checkbox"/>	<input type="checkbox"/>
1.34	Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	Ensure xinetd is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.1	Ensure time synchronization is in use	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.2	Ensure chrony is configured	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.3	Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.4	Ensure the operating system disables the chrony daemon from acting as a server	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.5	Ensure the operating system disables network management of the chrony daemon	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure X Window System is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure rsync service is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure Avahi Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure SNMP Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure HTTP Proxy Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Ensure Samba is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Ensure IMAP and POP3 server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	Ensure HTTP server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	Ensure FTP Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure DNS Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>

2.2.12	Ensure NFS is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure RPC is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	Ensure LDAP server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	Ensure DHCP Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	Ensure the telnet-server package is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.17	Ensure CUPS is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.18	Ensure NIS Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.19	Ensure mail transfer agent is configured for local-only mode	<input type="checkbox"/>	<input type="checkbox"/>
2.2.20	Ensure the operating system has enabled the hardware random number generator entropy gatherer service	<input type="checkbox"/>	<input type="checkbox"/>
2.2.21	Ensure automated bug reporting tools are not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.22	Ensure the sendmail package is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.23	Ensure the rsh-server package is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.24	Ensure a camera is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.25	Ensure the operating system is configured to mask the debug-shell systemd service	<input type="checkbox"/>	<input type="checkbox"/>
2.2.26	Ensure a TFTP server has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.27	Ensure the operating system is configured to prevent unrestricted mail relaying	<input type="checkbox"/>	<input type="checkbox"/>
2.2.28	Ensure the TFTP daemon is configured to operate in secure mode	<input type="checkbox"/>	<input type="checkbox"/>
2.2.29	Ensure an FTP server has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.30	Ensure the gssproxy package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.31	Ensure the iputils package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.32	Ensure the tuned package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.33	Ensure the krb5-server package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure NIS Client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure telnet client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure LDAP client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure IP forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure the system does not accept router advertisements on IPv6 interfaces, unless the system is a router	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure the system does not accept router advertisements on IPv6 interfaces by default, unless the system is a router	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>

3.2.7	Ensure Reverse Path Filtering is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.8	Ensure TCP SYN Cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.9	Ensure IPv6 router advertisements are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.10	Ensure the operating system does not accept IPv6 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.11	Ensure the operating system does not accept IPv6 source-routed packets	<input type="checkbox"/>	<input type="checkbox"/>
3.2.12	Ensure the operating system does not accept IPv6 source-routed packets by default	<input type="checkbox"/>	<input type="checkbox"/>
3.2.13	Ensure the operating system ignores IPv6 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.14	Ensure network interfaces are not in promiscuous mode	<input type="checkbox"/>	<input type="checkbox"/>
3.2.15	Ensure the operating system does not accept IPv4 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.16	Ensure the operating system does not accept IPv4 source-routed packet	<input type="checkbox"/>	<input type="checkbox"/>
3.2.17	Ensure the operating system does not accept IPv4 source-routed packets by default	<input type="checkbox"/>	<input type="checkbox"/>
3.2.18	Ensure the operating system ignores IPv4 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure DCCP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure SCTP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure RDS is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure TIPC is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure ATM is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure CAN is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.1	Ensure a Firewall package is installed	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.1	Ensure firewalld service is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure iptables service is not enabled with firewalld	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.3	Ensure nftables is not enabled with firewalld	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.4	Ensure firewalld default zone is set	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.5	Ensure network interfaces are assigned to appropriate zone	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.6	Ensure firewalld drops unnecessary services and ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.7	Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.8	Ensure "firewalld" is installed	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.1	Ensure iptables are flushed with nftables	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.2	Ensure an nftables table exists	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.3	Ensure nftables base chains exist	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.4	Ensure nftables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.5	Ensure nftables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.6	Ensure nftables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.7	Ensure nftables service is enabled	<input type="checkbox"/>	<input type="checkbox"/>

3.4.3.8	Ensure nftables rules are permanent	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.9	Ensure "nftables" is configured to allow rate limits on any connection to the system	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.1	Ensure iptables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.2	Ensure iptables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.3	Ensure iptables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.4	Ensure iptables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.5	Ensure iptables is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.1	Ensure ip6tables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.2	Ensure ip6tables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.3	Ensure ip6tables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.4	Ensure ip6tables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.5	Ensure ip6tables is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Disable IPv6	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure at least two name servers are configured if using DNS resolution	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure Bluetooth is disabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Ensure auditd is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Ensure auditd service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	Ensure audit_backlog_limit is sufficient	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.5	Ensure the audit service is configured to produce audit records	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.1	Ensure audit log storage size is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.2	Ensure audit logs are not automatically deleted	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.4	Ensure the operating system allocates audit record storage capacity	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.5	Ensure the operating system has the packages required for offloading audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.6	Ensure the operating system has the packages required for encrypting offloaded audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.7	Ensure the audit system off-loads audit records onto a different system or media from the system being audited	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.8	Ensure the audit system is configured to take an appropriate action when the internal event queue is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.9	Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.10	Ensure the operating system authenticates the remote logging server for off-loading audit logs	<input type="checkbox"/>	<input type="checkbox"/>

4.1.2.11	Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure changes to system administration scope (sudoers) is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure the SA and ISSO are notified in the event of an audit processing failure	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure the SA and ISSO are notified when the audit storage volume is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure an audit event is generated for any successful/unsuccessful use of the "chage" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure the operating system is configured to audit the execution of the "fremovexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.8	Ensure the operating system is configured to audit the execution of the "fsetxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.9	Ensure the operating system is configured to audit the execution of the "lsetxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.10	Ensure the operating system is configured to audit the execution of the "removexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.11	Ensure the operating system is configured to audit the execution of the "lremovexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.12	Ensure the operating system generates audit records when successful/unsuccessful attempts to use the "su" command by performing the following command to check the file system rules in "/etc/audit/audit.rules"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.13	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.14	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.15	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.16	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.17	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.18	Ensure the audit system prevents unauthorized changes to logon UIDs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.19	Ensure the audit system prevents unauthorized changes	<input type="checkbox"/>	<input type="checkbox"/>
4.1.20	Ensure the operating system takes the appropriate action when the audit storage volume is full	<input type="checkbox"/>	<input type="checkbox"/>

4.1.21	Ensure the operating system takes the appropriate action when the audit storage volume is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.22	Ensure login and logout events are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.23	Ensure the operating system takes the appropriate action when an audit processing failure occurs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.24	Ensure session initiation information is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.25	Ensure events that modify date and time information are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.26	Ensure events that modify the system's Mandatory Access Controls are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.27	Ensure events that modify the system's network environment are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.28	Ensure discretionary access control permission modification events are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.30	Ensure events that modify user/group information are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.31	Ensure successful file system mounts are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.32	Ensure use of privileged commands is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.34	Ensure kernel module loading and unloading is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.35	Ensure system administrator actions (sudolog) are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.36	Ensure the audit configuration is immutable	<input type="checkbox"/>	<input type="checkbox"/>
4.1.37	Ensure the operating system audits the execution of privileged functions	<input type="checkbox"/>	<input type="checkbox"/>
4.1.38	Ensure the operating system's audit daemon is configured to include local events	<input type="checkbox"/>	<input type="checkbox"/>
4.1.39	Ensure the operating system's audit daemon is configured to label all off-loaded audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.40	Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.41	Ensure the operating system's audit logs have a mode of "0600" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
4.1.42	Ensure the operating system's audit logs are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.43	Ensure the audit logs are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.44	Ensure the audit log directory is owned by "root" to prevent unauthorized read access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.45	Ensure the audit log directory is group-owned by "root" to prevent unauthorized read access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.46	Ensure the audit log directories have a mode of "0700" or less permissive by first determining where the audit logs are stored	<input type="checkbox"/>	<input type="checkbox"/>
4.1.47	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chcon" command	<input type="checkbox"/>	<input type="checkbox"/>

4.1.48	Ensure the operating system is configured to audit the execution of the "setxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.49	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.50	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.51	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-agent"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.52	Ensure an audit event is generated for any successful/unsuccessful use of the "passwd" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.53	Ensure an audit event is generated for any successful/unsuccessful use of the "mount" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.54	Ensure an audit event is generated for any successful/unsuccessful use of the "umount" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.55	Ensure an audit event is generated for any successful/unsuccessful use of the "mount" syscall	<input type="checkbox"/>	<input type="checkbox"/>
4.1.56	Ensure an audit event is generated for any successful/unsuccessful use of the "unix_update"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.57	Ensure an audit event is generated for any successful/unsuccessful use of "postdrop"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.58	Ensure an audit event is generated for any successful/unsuccessful use of "postqueue"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.59	Ensure an audit event is generated for any successful/unsuccessful use of "semanage"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.60	Ensure an audit event is generated for any successful/unsuccessful use of "setfiles"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.61	Ensure an audit event is generated for any successful/unsuccessful use of "userhelper"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.62	Ensure an audit event is generated for any successful/unsuccessful use of "setsebool"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.63	Ensure an audit event is generated for any successful/unsuccessful use of "unix_chkpwd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.64	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-keysign"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.65	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "setfacl" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.66	Ensure an audit event is generated for any successful/unsuccessful use of the "pam_timestamp_check" command	<input type="checkbox"/>	<input type="checkbox"/>

4.1.67	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "newgrp" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.68	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "init_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.69	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rename" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.70	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "renameat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.71	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rmdir" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.72	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlink" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.73	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlinkat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.74	Ensure an audit event is generated for any successful/unsuccessful use of the "gpasswd" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.75	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "finit_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.76	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "delete_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.77	Ensure an audit event is generated for any successful/unsuccessful use of the "crontab" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.78	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chsh" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.79	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "truncate" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.80	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "openat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.81	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.82	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open_by_handle_at" system call	<input type="checkbox"/>	<input type="checkbox"/>

4.1.83	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ftruncate" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.84	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "creat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.85	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chown" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.86	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chmod" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.87	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "lchown" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.88	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchownat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.89	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchown" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.90	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmod" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.91	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmodat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.92	Ensure an audit event is generated for any successful/unsuccessful use of the "sudo" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.93	Ensure an audit event is generated for any successful/unsuccessful use of the "usermod" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.94	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chacl" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.95	Ensure the operating system is configured to audit the execution of the module management program "kmod"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.96	Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "faillock" file occur	<input type="checkbox"/>	<input type="checkbox"/>
4.1.97	Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "lastlog" file	<input type="checkbox"/>	<input type="checkbox"/>
4.1.98	Ensure the operating system enables auditing of processes that start prior to the audit daemon	<input type="checkbox"/>	<input type="checkbox"/>

4.1.99	Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.100	Ensure the operating system enables Linux audit logging of the USBGuard daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.101	Ensure the files in directory "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
4.1.102	Ensure the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode	<input type="checkbox"/>	<input type="checkbox"/>
4.1.103	Ensure the audit tools are owned by "root" to prevent any unauthorized access, deletion, or modification	<input type="checkbox"/>	<input type="checkbox"/>
4.1.104	Ensure the audit tools are group-owned by "root" to prevent any unauthorized access, deletion, or modification	<input type="checkbox"/>	<input type="checkbox"/>
4.1.105	Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.1	Ensure rsyslog is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.3	Ensure the operating system monitors all remote access methods	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.4	Ensure rsyslog Service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.5	Ensure rsyslog default file permissions configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.6	Ensure logging is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.7	Ensure rsyslog is configured to send logs to a remote log host	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.8	Ensure remote rsyslog messages are only accepted on designated log hosts.	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.9	Ensure "rsyslog" is configured to log cron events	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.1	Ensure journald is configured to send logs to rsyslog	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.2	Ensure journald is configured to compress large log files	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure permissions on all logfiles are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure logrotate is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure administrators are notified if an audit processing failure occurs by modifying "/etc/aliases"	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure cron daemon is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure permissions on /etc/crontab are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on /etc/cron.hourly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure permissions on /etc/cron.daily are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure permissions on /etc/cron.weekly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure permissions on /etc/cron.monthly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure permissions on /etc/cron.d are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure SSH private key files have a passcode	<input type="checkbox"/>	<input type="checkbox"/>

5.2.3	Ensure SSH access is limited	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure permissions on SSH private host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure permissions on SSH public host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure SSH LogLevel is appropriate	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure SSH X11 forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	Ensure SSH IgnoreRhosts is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	Ensure SSH HostbasedAuthentication is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	Ensure SSH root login is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	Ensure SSH PermitEmptyPasswords is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.2.14	Ensure SSH PermitUserEnvironment is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.15	Ensure SSH Idle Timeout Interval is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.16	Ensure SSH LoginGraceTime is set to one minute or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.17	Ensure SSH warning banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.18	Ensure SSH PAM is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.19	Ensure SSH AllowTcpForwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.20	Ensure SSH MaxStartups is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.21	Ensure SSH MaxSessions is set to 4 or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.22	Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>
5.2.23	Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>
5.2.24	Ensure the SSH server uses strong entropy	<input type="checkbox"/>	<input type="checkbox"/>
5.2.25	Ensure system-wide crypto policy is not over-ridden	<input type="checkbox"/>	<input type="checkbox"/>
5.2.26	Ensure the SSH daemon performs strict mode checking of home directory configuration files	<input type="checkbox"/>	<input type="checkbox"/>
5.2.27	Ensure the SSH daemon performs compression after a user successfully authenticates	<input type="checkbox"/>	<input type="checkbox"/>
5.2.28	Ensure the SSH daemon does not allow authentication using known host's authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.29	Ensure the SSH daemon does not allow Kerberos authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.30	Ensure null passwords cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.2.31	Ensure SSH provides users with feedback on when account accesses last occurred	<input type="checkbox"/>	<input type="checkbox"/>
5.2.32	Ensure SSH is loaded and active	<input type="checkbox"/>	<input type="checkbox"/>
5.2.33	Ensure the SSH server is configured to force frequent session key renegotiation	<input type="checkbox"/>	<input type="checkbox"/>
5.2.34	Ensure the SSH daemon prevents remote hosts from connecting to the proxy display	<input type="checkbox"/>	<input type="checkbox"/>
5.2.35	Ensure system-wide crypto policies are in effect	<input type="checkbox"/>	<input type="checkbox"/>

5.2.36	Ensure the SSH daemon does not allow GSSAPI authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.37	Ensure SSH is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.2.38	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	Create custom authselect profile	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	Ensure authselect includes with-faillock	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1	Ensure password creation requirements are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2	Ensure the system locks an account after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3	Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts within 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.4	Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.5	Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.6	Ensure lockout for failed password attempts is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.8	Ensure password hashing algorithm is SHA-512	<input type="checkbox"/>	<input type="checkbox"/>
5.4.9	Ensure a minimum number of hash rounds is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.10	Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes until released by an administrator	<input type="checkbox"/>	<input type="checkbox"/>
5.4.11	Ensure the "/etc/security/faillock.conf" file is configured to lock an account until released by an administrator after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.12	Ensure the faillock directory contents persist after a reboot	<input type="checkbox"/>	<input type="checkbox"/>
5.4.13	Ensure the "/etc/security/faillock.conf" file is configured to use a non-default faillock directory to ensure contents persist after reboot	<input type="checkbox"/>	<input type="checkbox"/>
5.4.14	Ensure the system prevents informative messages to the user about logon information	<input type="checkbox"/>	<input type="checkbox"/>
5.4.15	Ensure the "/etc/security/faillock.conf" file is configured to prevent informative messages about logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.16	Ensure the system logs user name information when unsuccessful logon attempts occur	<input type="checkbox"/>	<input type="checkbox"/>
5.4.17	Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur	<input type="checkbox"/>	<input type="checkbox"/>
5.4.18	Ensure the system includes the root account when locking an account after three unsuccessful logon attempts within a period of 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>

5.4.19	Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur	<input type="checkbox"/>	<input type="checkbox"/>
5.4.21	Ensure the operating system uses multifactor authentication for local access to accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.22	Ensure the date and time of the last successful account logon upon logon is displayed	<input type="checkbox"/>	<input type="checkbox"/>
5.4.23	Ensure the "pam_unix.so" module is configured to use sha512	<input type="checkbox"/>	<input type="checkbox"/>
5.4.24	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/system-auth" file	<input type="checkbox"/>	<input type="checkbox"/>
5.4.25	Ensure blank or null passwords in the "system-auth" file cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.4.26	Ensure blank or null passwords in the "password-auth" file cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.4.27	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/password-auth" file	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.1	Ensure password expiration is 365 days or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.2	Ensure the shadow password suite configuration is set to encrypt password with a FIPS 140-2 approved cryptographic hashing algorithm.	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.3	Ensure the value of the "maxrepeat" option in "/etc/security/pwquality.conf" is "3"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.4	Ensure the value of the "difok" option in "/etc/security/pwquality.conf" is "8"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.5	Ensure the value of the "minclass" option in "/etc/security/pwquality.conf" is "4"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.6	Ensure the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" is "4"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.7	Ensure the value for "dcredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.8	Ensure the value for "lcredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.9	Ensure the value for "ucredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.10	Ensure the operating system uses "pwquality" to enforce the password complexity rules	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.11	Ensure minimum days between password changes is 7 or more	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.12	Ensure password expiration warning days is 7 or more	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.13	Ensure inactive password lock is 30 days or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.14	Ensure all users last password change date is in the past	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.15	Ensure the minimum time period between password changes for each user account is one day or greater	<input type="checkbox"/>	<input type="checkbox"/>

5.5.1.16	Ensure the operating system enforces 24 hours/1 day as the minimum password lifetime for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.17	Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.18	Ensure the maximum time period for existing passwords is restricted to 60 days	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.19	Ensure the operating system enforces a minimum 15-character password length	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.20	Ensure the operating system enforces a minimum 15-character password length for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.21	Ensure the value for "ocredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.22	Ensure the operating system prevents the use of dictionary words for passwords	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.23	Ensure the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt	<input type="checkbox"/>	<input type="checkbox"/>
5.5.3	Ensure default user shell timeout is 900 seconds or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.4	Ensure the interactive user account passwords are using a strong password hash	<input type="checkbox"/>	<input type="checkbox"/>
5.5.5	Ensure default group for the root account is GID 0	<input type="checkbox"/>	<input type="checkbox"/>
5.5.6	Ensure default user umask is 027 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
5.5.7	Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.5.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
5.5.9	Ensure the default umask for all local interactive users is "077"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.10	Ensure the umask default for installed shells is "077"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.11	Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files	<input type="checkbox"/>	<input type="checkbox"/>
5.6	Ensure root login is restricted to system console	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure PKI-based authentication has valid certificates	<input type="checkbox"/>	<input type="checkbox"/>
5.8	Ensure access to the su command is restricted	<input type="checkbox"/>	<input type="checkbox"/>
5.9	Ensure the operating system prevents system daemons from using Kerberos for authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.10	Ensure the krb5-workstation package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
5.11	Ensure SSSD prohibits the use of cached authentications after one day	<input type="checkbox"/>	<input type="checkbox"/>
5.12	Ensure "fapolicyd" is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.13	Ensure USBGuard has a policy configured	<input type="checkbox"/>	<input type="checkbox"/>
5.14	Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>

5.15	Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption	<input type="checkbox"/>	<input type="checkbox"/>
5.16	Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions	<input type="checkbox"/>	<input type="checkbox"/>
5.17	Ensure "fapolicyd" is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
5.18	Ensure "fapolicyd" employs a deny-all, permit-by-exception policy	<input type="checkbox"/>	<input type="checkbox"/>
5.19	Ensure USBGuard is installed on the operating system	<input type="checkbox"/>	<input type="checkbox"/>
5.20	Ensure the operating system has enabled the use of the USBGuard	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Audit system file permissions	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure permissions on /etc/passwd are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Ensure permissions on /etc/passwd- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.4	Ensure permissions on /etc/shadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.5	Ensure permissions on /etc/shadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.6	Ensure permissions on /etc/gshadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.7	Ensure permissions on /etc/gshadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.8	Ensure permissions on /etc/group are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.9	Ensure permissions on /etc/group- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.10	Ensure the root account is the only account that has unrestricted access to the operating system	<input type="checkbox"/>	<input type="checkbox"/>
6.1.11	Ensure no world writable files exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.12	Ensure no unowned files or directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.13	Ensure no ungrouped files or directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.14	Ensure all public directories are owned by root or a system account	<input type="checkbox"/>	<input type="checkbox"/>
6.1.15	Audit SUID executables	<input type="checkbox"/>	<input type="checkbox"/>
6.1.16	Audit SGID executables	<input type="checkbox"/>	<input type="checkbox"/>
6.1.17	Ensure the "/var/log/messages" file has mode "0640" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.18	Ensure the "/var/log/messages" file is owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.19	Ensure the "/var/log/messages" file is group-owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.20	Ensure the "/var/log" directory has a mode of "0755" or less	<input type="checkbox"/>	<input type="checkbox"/>
6.1.21	Ensure the "/var/log" directory is owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.22	Ensure the "/var/log" directory is group-owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.23	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories have mode "0755" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.24	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.25	Ensure the system commands contained in "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>

6.1.26	Ensure the system-wide shared library files contained in the "/lib, /lib64, /usr/lib, /usr/lib64" directories have mode "0755" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.27	Ensure the system-wide shared library files are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.28	Ensure the system-wide shared library files are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.29	Ensure world-writable directories are owned by root, sys, bin, or an application user	<input type="checkbox"/>	<input type="checkbox"/>
6.1.30	Ensure world-writable directories are group-owned by root, sys, bin, or an application group	<input type="checkbox"/>	<input type="checkbox"/>
6.1.31	Ensure local initialization files do not execute world-writable programs	<input type="checkbox"/>	<input type="checkbox"/>
6.1.32	Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer	<input type="checkbox"/>	<input type="checkbox"/>
6.1.33	Ensure the operating system prevents users from disabling the tmux terminal multiplexer	<input type="checkbox"/>	<input type="checkbox"/>
6.1.34	Ensure the operating system enables a user's session lock until that user re-establishes access	<input type="checkbox"/>	<input type="checkbox"/>
6.1.35	Ensure the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
6.1.36	Ensure the operating system initiates a session lock after 15 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
6.1.37	Ensure all accounts on the system are assigned to an active system, application, or user account	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1	Ensure password fields are not empty	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Ensure root PATH Integrity	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Ensure no legacy "+" entries exist in /etc/shadow	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure no legacy "+" entries exist in /etc/group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure root is the only UID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure users' home directories permissions are 750 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
6.2.9	Ensure users own their home directories	<input type="checkbox"/>	<input type="checkbox"/>
6.2.10	Ensure users' dot files are not group or world writable	<input type="checkbox"/>	<input type="checkbox"/>
6.2.11	Ensure no users have .forward files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.12	Ensure no users have .netrc files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.13	Ensure users' .netrc Files are not group or world accessible	<input type="checkbox"/>	<input type="checkbox"/>
6.2.14	Ensure no users have .rhosts files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.20	Ensure shadow group is empty	<input type="checkbox"/>	<input type="checkbox"/>
6.2.21	Ensure all users' home directories exist	<input type="checkbox"/>	<input type="checkbox"/>

6.2.22	Ensure the assigned home directory of all local interactive users is group-owned by that user's primary GID	<input type="checkbox"/>	<input type="checkbox"/>
6.2.23	Ensure the assigned home directory of all local interactive users exists	<input type="checkbox"/>	<input type="checkbox"/>
6.2.24	Ensure all local interactive users are assigned a home directory upon creation	<input type="checkbox"/>	<input type="checkbox"/>
6.2.25	Ensure all local initialization files have a mode of "0740" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.2.26	Ensure all local files and directories have a valid owner	<input type="checkbox"/>	<input type="checkbox"/>
6.2.27	Ensure all local files and directories have a valid group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.28	Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file	<input type="checkbox"/>	<input type="checkbox"/>
6.2.29	Ensure file executable search path statements do not share sensitive home directory information	<input type="checkbox"/>	<input type="checkbox"/>
6.2.30	Ensure local interactive users have a home directory assigned	<input type="checkbox"/>	<input type="checkbox"/>
6.2.31	Ensure the operating system limits the number of concurrent sessions to "10" for all accounts and/or account types	<input type="checkbox"/>	<input type="checkbox"/>
6.2.32	Ensure the operating system enables a user's session lock until that user re-establishes access	<input type="checkbox"/>	<input type="checkbox"/>
6.2.33	Ensure the operating system enables the user to initiate a session lock	<input type="checkbox"/>	<input type="checkbox"/>
6.2.34	Ensure the operating system prevents a user from overriding settings for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
6.2.35	Ensure all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750"	<input type="checkbox"/>	<input type="checkbox"/>
6.2.36	Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of	<input type="checkbox"/>	<input type="checkbox"/>
6.2.37	Ensure temporary accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure the operating system removes all software components after updated versions have been installed	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure there are no ".shosts" files on the operating system	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Ensure there are no "shosts.equiv" files on the operating system	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of cramfs filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure mounting of vFAT filesystems is limited	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure mounting of squashfs filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure mounting of udf filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Ensure /tmp is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Ensure nodev option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Ensure nosuid option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Ensure noexec option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	Ensure separate partition exists for /var	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Ensure separate partition exists for /var/tmp	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Ensure nodev option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Ensure nosuid option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Ensure noexec option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.11	Ensure separate partition exists for /var/log	<input type="checkbox"/>	<input type="checkbox"/>
1.1.12	Ensure separate partition exists for /var/log/audit	<input type="checkbox"/>	<input type="checkbox"/>
1.1.13	Ensure separate partition exists for /home	<input type="checkbox"/>	<input type="checkbox"/>
1.1.14	Ensure nodev option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.15	Ensure nodev option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.16	Ensure nosuid option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.17	Ensure noexec option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.18	Ensure nodev option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.19	Ensure nosuid option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.20	Ensure noexec option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.21	Ensure sticky bit is set on all world-writable directories	<input type="checkbox"/>	<input type="checkbox"/>
1.1.22	Disable Automounting	<input type="checkbox"/>	<input type="checkbox"/>
1.1.23	Disable USB Storage	<input type="checkbox"/>	<input type="checkbox"/>
1.1.24	Ensure file systems that contain user home directories are mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.25	Ensure the "/boot" directory is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.26	Ensure all non-root local partitions are mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.27	Ensure file systems that are being NFS-imported are mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.29	Ensure file systems being imported via NFS are mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>

1.1.30	Ensure a separate file system/partition has been created for non-privileged local interactive user home directories	<input type="checkbox"/>	<input type="checkbox"/>
1.1.31	Ensure "/var/log" is mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.32	Ensure "/var/log" is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.33	Ensure "/var/log" is mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.34	Ensure "/var/log/audit" is mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.35	Ensure "/var/log/audit" is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.36	Ensure "/var/log/audit" is mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.37	Ensure the "/boot/efi" directory is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.38	Ensure file systems that contain user home directories are mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1	Ensure GPG keys are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Ensure gpgcheck is globally activated	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Ensure package manager repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Ensure DNF is configured to perform a signature check on local packages	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Ensure sudo is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
1.3.3	Ensure sudo log file exists	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Ensure the "/etc/sudoers" file has no occurrences of "NOPASSWD"	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	Ensure the "/etc/sudoers" file has no occurrences of "!authenticate"	<input type="checkbox"/>	<input type="checkbox"/>
1.3.6	Ensure the "sudoers" file restricts sudo access to authorized personnel	<input type="checkbox"/>	<input type="checkbox"/>
1.3.7	Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation	<input type="checkbox"/>	<input type="checkbox"/>
1.3.8	Ensure the operating system requires re-authentication when using the "sudo" command to elevate privileges	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure AIDE is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure filesystem integrity is regularly checked	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Ensure Advanced Intrusion Detection Environment (AIDE) is properly configured to use cryptographic mechanisms to protect the integrity of audit tools	<input type="checkbox"/>	<input type="checkbox"/>
1.4.4	Ensure the file integrity tool is configured to verify extended attributes	<input type="checkbox"/>	<input type="checkbox"/>
1.4.5	Ensure the file integrity tool is configured to verify ACLs	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure permissions on bootloader config are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure bootloader password is set	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Ensure authentication required for single user mode	<input type="checkbox"/>	<input type="checkbox"/>

1.5.4	Ensure the encrypted grub superusers password is set for systems booted with UEFI	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Ensure the encrypted grub superusers password is set for system booted with BIOS	<input type="checkbox"/>	<input type="checkbox"/>
1.5.6	Ensure the operating system requires authentication for rescue mode	<input type="checkbox"/>	<input type="checkbox"/>
1.5.7	Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities	<input type="checkbox"/>	<input type="checkbox"/>
1.5.8	Ensure GRUB 2 is configured to disable vsyscalls	<input type="checkbox"/>	<input type="checkbox"/>
1.5.9	Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities	<input type="checkbox"/>	<input type="checkbox"/>
1.5.10	Ensure the operating system is configured to boot to the command line	<input type="checkbox"/>	<input type="checkbox"/>
1.5.11	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed	<input type="checkbox"/>	<input type="checkbox"/>
1.5.12	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds	<input type="checkbox"/>	<input type="checkbox"/>
1.5.13	Ensure a unique name is set as the "superusers" account (UEFI)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.14	Ensure a unique name is set as the "superusers" account (BIOS)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.15	Ensure the operating system requires authentication upon booting into emergency mode	<input type="checkbox"/>	<input type="checkbox"/>
1.6.1	Ensure core dumps are restricted	<input type="checkbox"/>	<input type="checkbox"/>
1.6.2	Ensure address space layout randomization (ASLR) is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure the operating system is not configured to acquire, save, or process core dumps	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure kernel core dumps are disabled unless needed	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure the operating system disables core dumps for all users	<input type="checkbox"/>	<input type="checkbox"/>
1.6.7	Ensure the operating system disables storing core dumps for all users	<input type="checkbox"/>	<input type="checkbox"/>
1.6.8	Ensure the operating system disables core dump backtraces	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.1	Ensure SELinux is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.2	Ensure SELinux is not disabled in bootloader configuration	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.3	Ensure SELinux policy is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.4	Ensure the SELinux state is enforcing	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.5	Ensure no unconfined services exist	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.6	Ensure SETroubleshoot is not installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.7	Ensure the MCS Translation Service (mcstrans) is not installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.8	Ensure the operating system has the policycoreutils package installed	<input type="checkbox"/>	<input type="checkbox"/>

1.8.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.8.2	Ensure message of the day is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.3	Ensure local login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.4	Ensure remote login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.5	Ensure permissions on /etc/motd are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.6	Ensure permissions on /etc/issue are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.7	Ensure permissions on /etc/issue.net are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.8	Ensure the Standard Mandatory DoD Notice and Consent Banner is displayed before granting access to the system via SSH logon	<input type="checkbox"/>	<input type="checkbox"/>
1.8.9	Ensure the operating system displays a banner before granting access to the operating system via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.2	Ensure GNOME Display Manager is removed	<input type="checkbox"/>	<input type="checkbox"/>
1.9.3	Ensure GDM login banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.9.4	Ensure last logged in user display is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.9.5	Ensure XDCMP is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.9.6	Ensure a Standard Mandatory DoD Notice and Consent Banner is displayed via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.7	Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.8	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.9	Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated	<input type="checkbox"/>	<input type="checkbox"/>
1.9.10	Ensure the operating system disables the user logon list for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
1.9.11	Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.12	Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.10	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure system-wide crypto policy is not legacy	<input type="checkbox"/>	<input type="checkbox"/>
1.12	Ensure system-wide crypto policy is FUTURE or FIPS	<input type="checkbox"/>	<input type="checkbox"/>

1.13	Ensure the operating system implements DoD-approved encryption	<input type="checkbox"/>	<input type="checkbox"/>
1.14	Ensure the operating system prevents unauthorized modification of all information at rest by using disk encryption	<input type="checkbox"/>	<input type="checkbox"/>
1.15	Ensure kernel image loading is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure the operating system is configured to enable DAC on symlinks	<input type="checkbox"/>	<input type="checkbox"/>
1.17	Ensure the operating system is configured to enable DAC on hardlinks	<input type="checkbox"/>	<input type="checkbox"/>
1.18	Ensure the operating system is configured to restrict access to the kernel message buffer	<input type="checkbox"/>	<input type="checkbox"/>
1.19	Ensure the operating system is configured to prevent kernel profiling by unprivileged users	<input type="checkbox"/>	<input type="checkbox"/>
1.20	Ensure the operating system has the packages required for multifactor authentication	<input type="checkbox"/>	<input type="checkbox"/>
1.22	Ensure the operating system accepts PIV credentials	<input type="checkbox"/>	<input type="checkbox"/>
1.23	Ensure the NX (no-execution) bit flag is set on the system	<input type="checkbox"/>	<input type="checkbox"/>
1.24	Ensure kernel page-table isolation is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.25	Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall	<input type="checkbox"/>	<input type="checkbox"/>
1.26	Ensure the operating system restricts usage of ptrace to descendant processes	<input type="checkbox"/>	<input type="checkbox"/>
1.27	Ensure the operating system restricts exposed kernel pointer addresses access	<input type="checkbox"/>	<input type="checkbox"/>
1.28	Ensure the operating system disables the ability to load the firewire-core kernel module	<input type="checkbox"/>	<input type="checkbox"/>
1.29	Ensure the operating system disables the ability to load the USB Storage kernel module	<input type="checkbox"/>	<input type="checkbox"/>
1.30	Ensure the operating system disables the use of user namespaces	<input type="checkbox"/>	<input type="checkbox"/>
1.31	Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service	<input type="checkbox"/>	<input type="checkbox"/>
1.32	Ensure the "tmux" package installed	<input type="checkbox"/>	<input type="checkbox"/>
1.33	Ensure the operating system enables hardening for the BPF JIT	<input type="checkbox"/>	<input type="checkbox"/>
1.34	Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	Ensure xinetd is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.1	Ensure time synchronization is in use	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.2	Ensure chrony is configured	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.3	Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server	<input type="checkbox"/>	<input type="checkbox"/>

2.2.1.4	Ensure the operating system disables the chrony daemon from acting as a server	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.5	Ensure the operating system disables network management of the chrony daemon	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure X Window System is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure rsync service is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure Avahi Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure SNMP Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure HTTP Proxy Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Ensure Samba is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Ensure IMAP and POP3 server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	Ensure HTTP server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	Ensure FTP Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure DNS Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.12	Ensure NFS is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure RPC is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	Ensure LDAP server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	Ensure DHCP Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	Ensure the telnet-server package is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.17	Ensure CUPS is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.18	Ensure NIS Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.19	Ensure mail transfer agent is configured for local-only mode	<input type="checkbox"/>	<input type="checkbox"/>
2.2.20	Ensure the operating system has enabled the hardware random number generator entropy gatherer service	<input type="checkbox"/>	<input type="checkbox"/>
2.2.21	Ensure automated bug reporting tools are not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.22	Ensure the sendmail package is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.23	Ensure the rsh-server package is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.24	Ensure a camera is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.25	Ensure the operating system is configured to mask the debug-shell systemd service	<input type="checkbox"/>	<input type="checkbox"/>
2.2.26	Ensure a TFTP server has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.27	Ensure the operating system is configured to prevent unrestricted mail relaying	<input type="checkbox"/>	<input type="checkbox"/>
2.2.28	Ensure the TFTP daemon is configured to operate in secure mode	<input type="checkbox"/>	<input type="checkbox"/>
2.2.29	Ensure an FTP server has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.30	Ensure the gssproxy package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.31	Ensure the iputils package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.32	Ensure the tuned package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.33	Ensure the krb5-server package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure NIS Client is not installed	<input type="checkbox"/>	<input type="checkbox"/>

2.3.2	Ensure telnet client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure LDAP client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure IP forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure the system does not accept router advertisements on IPv6 interfaces, unless the system is a router	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure the system does not accept router advertisements on IPv6 interfaces by default, unless the system is a router	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure Reverse Path Filtering is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.8	Ensure TCP SYN Cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.9	Ensure IPv6 router advertisements are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.10	Ensure the operating system does not accept IPv6 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.11	Ensure the operating system does not accept IPv6 source-routed packets	<input type="checkbox"/>	<input type="checkbox"/>
3.2.12	Ensure the operating system does not accept IPv6 source-routed packets by default	<input type="checkbox"/>	<input type="checkbox"/>
3.2.13	Ensure the operating system ignores IPv6 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.14	Ensure network interfaces are not in promiscuous mode	<input type="checkbox"/>	<input type="checkbox"/>
3.2.15	Ensure the operating system does not accept IPv4 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.16	Ensure the operating system does not accept IPv4 source-routed packet	<input type="checkbox"/>	<input type="checkbox"/>
3.2.17	Ensure the operating system does not accept IPv4 source-routed packets by default	<input type="checkbox"/>	<input type="checkbox"/>
3.2.18	Ensure the operating system ignores IPv4 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure DCCP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure SCTP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure RDS is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure TIPC is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure ATM is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure CAN is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.1	Ensure a Firewall package is installed	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.1	Ensure firewalld service is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure iptables service is not enabled with firewalld	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.3	Ensure nftables is not enabled with firewalld	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.4	Ensure firewalld default zone is set	<input type="checkbox"/>	<input type="checkbox"/>

3.4.2.5	Ensure network interfaces are assigned to appropriate zone	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.6	Ensure firewalld drops unnecessary services and ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.7	Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.8	Ensure "firewalld" is installed	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.1	Ensure iptables are flushed with nftables	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.2	Ensure an nftables table exists	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.3	Ensure nftables base chains exist	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.4	Ensure nftables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.5	Ensure nftables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.6	Ensure nftables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.7	Ensure nftables service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.8	Ensure nftables rules are permanent	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.9	Ensure "nftables" is configured to allow rate limits on any connection to the system	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.1	Ensure iptables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.2	Ensure iptables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.3	Ensure iptables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.4	Ensure iptables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.5	Ensure iptables is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.1	Ensure ip6tables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.2	Ensure ip6tables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.3	Ensure ip6tables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.4	Ensure ip6tables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.5	Ensure ip6tables is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Ensure wireless interfaces are disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Disable IPv6	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure at least two name servers are configured if using DNS resolution	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure Bluetooth is disabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Ensure auditd is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Ensure auditd service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	Ensure audit_backlog_limit is sufficient	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.5	Ensure the audit service is configured to produce audit records	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.1	Ensure audit log storage size is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.2	Ensure audit logs are not automatically deleted	<input type="checkbox"/>	<input type="checkbox"/>

4.1.2.4	Ensure the operating system allocates audit record storage capacity	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.5	Ensure the operating system has the packages required for offloading audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.6	Ensure the operating system has the packages required for encrypting offloaded audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.7	Ensure the audit system off-loads audit records onto a different system or media from the system being audited	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.8	Ensure the audit system is configured to take an appropriate action when the internal event queue is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.9	Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.10	Ensure the the operating system authenticates the remote logging server for off-loading audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.11	Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure changes to system administration scope (sudoers) is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure the SA and ISSO are notified in the event of an audit processing failure	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure the SA and ISSO are notified when the audit storage volume is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure an audit event is generated for any successful/unsuccessful use of the "chage" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure the operating system is configured to audit the execution of the "fremovexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.8	Ensure the operating system is configured to audit the execution of the "fsetxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.9	Ensure the operating system is configured to audit the execution of the "lsetxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.10	Ensure the operating system is configured to audit the execution of the "removexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.11	Ensure the operating system is configured to audit the execution of the "lremovexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.12	Ensure the operating system generates audit records when successful/unsuccessful attempts to use the "su" command by performing the following command to check the file system rules in "/etc/audit/audit.rules"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.13	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.14	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers"	<input type="checkbox"/>	<input type="checkbox"/>

4.1.15	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.16	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.17	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.18	Ensure the audit system prevents unauthorized changes to logon UIDs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.19	Ensure the audit system prevents unauthorized changes	<input type="checkbox"/>	<input type="checkbox"/>
4.1.20	Ensure the operating system takes the appropriate action when the audit storage volume is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.21	Ensure the operating system takes the appropriate action when the audit storage volume is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.22	Ensure login and logout events are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.23	Ensure the operating system takes the appropriate action when an audit processing failure occurs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.24	Ensure session initiation information is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.25	Ensure events that modify date and time information are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.26	Ensure events that modify the system's Mandatory Access Controls are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.27	Ensure events that modify the system's network environment are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.28	Ensure discretionary access control permission modification events are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.29	Ensure unsuccessful unauthorized file access attempts are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.30	Ensure events that modify user/group information are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.31	Ensure successful file system mounts are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.32	Ensure use of privileged commands is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.34	Ensure kernel module loading and unloading is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.35	Ensure system administrator actions (sudolog) are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.36	Ensure the audit configuration is immutable	<input type="checkbox"/>	<input type="checkbox"/>
4.1.37	Ensure the operating system audits the execution of privileged functions	<input type="checkbox"/>	<input type="checkbox"/>
4.1.38	Ensure the operating system's audit daemon is configured to include local events	<input type="checkbox"/>	<input type="checkbox"/>
4.1.39	Ensure the operating system's audit daemon is configured to label all off-loaded audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.40	Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk	<input type="checkbox"/>	<input type="checkbox"/>

4.1.41	Ensure the operating system's audit logs have a mode of "0600" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
4.1.42	Ensure the operating system's audit logs are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.43	Ensure the audit logs are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.44	Ensure the audit log directory is owned by "root" to prevent unauthorized read access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.45	Ensure the audit log directory is group-owned by "root" to prevent unauthorized read access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.46	Ensure the audit log directories have a mode of "0700" or less permissive by first determining where the audit logs are stored	<input type="checkbox"/>	<input type="checkbox"/>
4.1.47	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chcon" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.48	Ensure the operating system is configured to audit the execution of the "setxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.49	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.50	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.51	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-agent"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.52	Ensure an audit event is generated for any successful/unsuccessful use of the "passwd" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.53	Ensure an audit event is generated for any successful/unsuccessful use of the "mount" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.54	Ensure an audit event is generated for any successful/unsuccessful use of the "umount" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.55	Ensure an audit event is generated for any successful/unsuccessful use of the "mount" syscall	<input type="checkbox"/>	<input type="checkbox"/>
4.1.56	Ensure an audit event is generated for any successful/unsuccessful use of the "unix_update"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.57	Ensure an audit event is generated for any successful/unsuccessful use of "postdrop"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.58	Ensure an audit event is generated for any successful/unsuccessful use of "postqueue"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.59	Ensure an audit event is generated for any successful/unsuccessful use of "semanage"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.60	Ensure an audit event is generated for any successful/unsuccessful use of "setfiles"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.61	Ensure an audit event is generated for any successful/unsuccessful use of "userhelper"	<input type="checkbox"/>	<input type="checkbox"/>

4.1.62	Ensure an audit event is generated for any successful/unsuccessful use of "setsebool"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.63	Ensure an audit event is generated for any successful/unsuccessful use of "unix_chkpwd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.64	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-keysign"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.65	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "setfacl" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.66	Ensure an audit event is generated for any successful/unsuccessful use of the "pam_timestamp_check" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.67	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "newgrp" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.68	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "init_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.69	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rename" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.70	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "renameat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.71	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rmdir" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.72	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlink" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.73	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlinkat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.74	Ensure an audit event is generated for any successful/unsuccessful use of the "gpasswd" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.75	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "finit_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.76	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "delete_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.77	Ensure an audit event is generated for any successful/unsuccessful use of the "crontab" command	<input type="checkbox"/>	<input type="checkbox"/>

4.1.78	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chsh" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.79	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "truncate" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.80	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "openat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.81	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.82	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open_by_handle_at" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.83	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ftruncate" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.84	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "creat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.85	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chown" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.86	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chmod" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.87	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "lchown" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.88	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchownat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.89	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchown" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.90	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmod" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.91	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmodat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.92	Ensure an audit event is generated for any successful/unsuccessful use of the "sudo" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.93	Ensure an audit event is generated for any successful/unsuccessful use of the "usermod" command	<input type="checkbox"/>	<input type="checkbox"/>

4.1.94	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chacl" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.95	Ensure the operating system is configured to audit the execution of the module management program "kmod"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.96	Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "faillock" file occur	<input type="checkbox"/>	<input type="checkbox"/>
4.1.97	Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "lastlog" file	<input type="checkbox"/>	<input type="checkbox"/>
4.1.98	Ensure the operating system enables auditing of processes that start prior to the audit daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.99	Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.100	Ensure the operating system enables Linux audit logging of the USBGuard daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.101	Ensure the files in directory "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
4.1.102	Ensure the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode	<input type="checkbox"/>	<input type="checkbox"/>
4.1.103	Ensure the audit tools are owned by "root" to prevent any unauthorized access, deletion, or modification	<input type="checkbox"/>	<input type="checkbox"/>
4.1.104	Ensure the audit tools are group-owned by "root" to prevent any unauthorized access, deletion, or modification	<input type="checkbox"/>	<input type="checkbox"/>
4.1.105	Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.1	Ensure rsyslog is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.3	Ensure the operating system monitors all remote access methods	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.4	Ensure rsyslog Service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.5	Ensure rsyslog default file permissions configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.6	Ensure logging is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.7	Ensure rsyslog is configured to send logs to a remote log host	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.8	Ensure remote rsyslog messages are only accepted on designated log hosts.	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.9	Ensure "rsyslog" is configured to log cron events	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.1	Ensure journald is configured to send logs to rsyslog	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.2	Ensure journald is configured to compress large log files	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk	<input type="checkbox"/>	<input type="checkbox"/>

4.2.3	Ensure permissions on all logfiles are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure logrotate is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure administrators are notified if an audit processing failure occurs by modifying "/etc/aliases"	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure cron daemon is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure permissions on /etc/crontab are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on /etc/cron.hourly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure permissions on /etc/cron.daily are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure permissions on /etc/cron.weekly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure permissions on /etc/cron.monthly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure permissions on /etc/cron.d are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure SSH private key files have a passcode	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure SSH access is limited	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure permissions on SSH private host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure permissions on SSH public host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure SSH LogLevel is appropriate	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure SSH X11 forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	Ensure SSH MaxAuthTries is set to 4 or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	Ensure SSH IgnoreRhosts is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	Ensure SSH HostbasedAuthentication is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	Ensure SSH root login is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	Ensure SSH PermitEmptyPasswords is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.2.14	Ensure SSH PermitUserEnvironment is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.15	Ensure SSH Idle Timeout Interval is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.16	Ensure SSH LoginGraceTime is set to one minute or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.17	Ensure SSH warning banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.18	Ensure SSH PAM is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.19	Ensure SSH AllowTcpForwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.20	Ensure SSH MaxStartups is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.21	Ensure SSH MaxSessions is set to 4 or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.22	Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>
5.2.23	Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>
5.2.24	Ensure the SSH server uses strong entropy	<input type="checkbox"/>	<input type="checkbox"/>
5.2.25	Ensure system-wide crypto policy is not over-ridden	<input type="checkbox"/>	<input type="checkbox"/>
5.2.26	Ensure the SSH daemon performs strict mode checking of home directory configuration files	<input type="checkbox"/>	<input type="checkbox"/>

5.2.27	Ensure the SSH daemon performs compression after a user successfully authenticates	<input type="checkbox"/>	<input type="checkbox"/>
5.2.28	Ensure the SSH daemon does not allow authentication using known host's authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.29	Ensure the SSH daemon does not allow Kerberos authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.30	Ensure null passwords cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.2.31	Ensure SSH provides users with feedback on when account accesses last occurred	<input type="checkbox"/>	<input type="checkbox"/>
5.2.32	Ensure SSH is loaded and active	<input type="checkbox"/>	<input type="checkbox"/>
5.2.33	Ensure the SSH server is configured to force frequent session key renegotiation	<input type="checkbox"/>	<input type="checkbox"/>
5.2.34	Ensure the SSH daemon prevents remote hosts from connecting to the proxy display	<input type="checkbox"/>	<input type="checkbox"/>
5.2.35	Ensure system-wide crypto policies are in effect	<input type="checkbox"/>	<input type="checkbox"/>
5.2.36	Ensure the SSH daemon does not allow GSSAPI authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.37	Ensure SSH is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.2.38	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	Create custom authselect profile	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	Ensure authselect includes with-faillock	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1	Ensure password creation requirements are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2	Ensure the system locks an account after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3	Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts within 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.4	Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.5	Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.6	Ensure lockout for failed password attempts is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.8	Ensure password hashing algorithm is SHA-512	<input type="checkbox"/>	<input type="checkbox"/>
5.4.9	Ensure a minimum number of hash rounds is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.10	Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes until released by an administrator	<input type="checkbox"/>	<input type="checkbox"/>
5.4.11	Ensure the "/etc/security/faillock.conf" file is configured to lock an account until released by an administrator after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.12	Ensure the faillock directory contents persist after a reboot	<input type="checkbox"/>	<input type="checkbox"/>

5.4.13	Ensure the "/etc/security/faillock.conf" file is configured to use a non-default faillock directory to ensure contents persist after reboot	<input type="checkbox"/>	<input type="checkbox"/>
5.4.14	Ensure the system prevents informative messages to the user about logon information	<input type="checkbox"/>	<input type="checkbox"/>
5.4.15	Ensure the "/etc/security/faillock.conf" file is configured to prevent informative messages about logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.16	Ensure the system logs user name information when unsuccessful logon attempts occur	<input type="checkbox"/>	<input type="checkbox"/>
5.4.17	Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur	<input type="checkbox"/>	<input type="checkbox"/>
5.4.18	Ensure the system includes the root account when locking an account after three unsuccessful logon attempts within a period of 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.19	Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur	<input type="checkbox"/>	<input type="checkbox"/>
5.4.21	Ensure the operating system uses multifactor authentication for local access to accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.22	Ensure the date and time of the last successful account logon upon logon is displayed	<input type="checkbox"/>	<input type="checkbox"/>
5.4.23	Ensure the "pam_unix.so" module is configured to use sha512	<input type="checkbox"/>	<input type="checkbox"/>
5.4.24	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/system-auth" file	<input type="checkbox"/>	<input type="checkbox"/>
5.4.25	Ensure blank or null passwords in the "system-auth" file cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.4.26	Ensure blank or null passwords in the "password-auth" file cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.4.27	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/password-auth" file	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.1	Ensure password expiration is 365 days or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.2	Ensure the shadow password suite configuration is set to encrypt password with a FIPS 140-2 approved cryptographic hashing algorithm.	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.3	Ensure the value of the "maxrepeat" option in "/etc/security/pwquality.conf" is "3"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.4	Ensure the value of the "difok" option in "/etc/security/pwquality.conf" is "8"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.5	Ensure the value of the "minclass" option in "/etc/security/pwquality.conf" is "4"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.6	Ensure the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" is "4"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.7	Ensure the value for "dcredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>

5.5.1.8	Ensure the value for "lcredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.9	Ensure the value for "ucredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.10	Ensure the operating system uses "pwquality" to enforce the password complexity rules	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.11	Ensure minimum days between password changes is 7 or more	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.12	Ensure password expiration warning days is 7 or more	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.13	Ensure inactive password lock is 30 days or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.14	Ensure all users last password change date is in the past	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.15	Ensure the minimum time period between password changes for each user account is one day or greater	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.16	Ensure the operating system enforces 24 hours/1 day as the minimum password lifetime for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.17	Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.18	Ensure the maximum time period for existing passwords is restricted to 60 days	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.19	Ensure the operating system enforces a minimum 15-character password length	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.20	Ensure the operating system enforces a minimum 15-character password length for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.21	Ensure the value for "ocredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.22	Ensure the operating system prevents the use of dictionary words for passwords	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.23	Ensure the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt	<input type="checkbox"/>	<input type="checkbox"/>
5.5.3	Ensure default user shell timeout is 900 seconds or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.4	Ensure the interactive user account passwords are using a strong password hash	<input type="checkbox"/>	<input type="checkbox"/>
5.5.5	Ensure default group for the root account is GID 0	<input type="checkbox"/>	<input type="checkbox"/>
5.5.6	Ensure default user umask is 027 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
5.5.7	Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.5.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
5.5.9	Ensure the default umask for all local interactive users is "077"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.10	Ensure the umask default for installed shells is "077"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.11	Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files	<input type="checkbox"/>	<input type="checkbox"/>

5.6	Ensure root login is restricted to system console	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure PKI-based authentication has valid certificates	<input type="checkbox"/>	<input type="checkbox"/>
5.8	Ensure access to the su command is restricted	<input type="checkbox"/>	<input type="checkbox"/>
5.9	Ensure the operating system prevents system daemons from using Kerberos for authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.10	Ensure the krb5-workstation package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
5.11	Ensure SSSD prohibits the use of cached authentications after one day	<input type="checkbox"/>	<input type="checkbox"/>
5.12	Ensure "fapolicyd" is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.13	Ensure USGuard has a policy configured	<input type="checkbox"/>	<input type="checkbox"/>
5.14	Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>
5.15	Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption	<input type="checkbox"/>	<input type="checkbox"/>
5.16	Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions	<input type="checkbox"/>	<input type="checkbox"/>
5.17	Ensure "fapolicyd" is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
5.18	Ensure "fapolicyd" employs a deny-all, permit-by-exception policy	<input type="checkbox"/>	<input type="checkbox"/>
5.19	Ensure USGuard is installed on the operating system	<input type="checkbox"/>	<input type="checkbox"/>
5.20	Ensure the operating system has enabled the use of the USGuard	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Audit system file permissions	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure permissions on /etc/passwd are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Ensure permissions on /etc/passwd- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.4	Ensure permissions on /etc/shadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.5	Ensure permissions on /etc/shadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.6	Ensure permissions on /etc/gshadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.7	Ensure permissions on /etc/gshadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.8	Ensure permissions on /etc/group are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.9	Ensure permissions on /etc/group- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.10	Ensure the root account is the only account that has unrestricted access to the operating system	<input type="checkbox"/>	<input type="checkbox"/>
6.1.11	Ensure no world writable files exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.12	Ensure no unowned files or directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.13	Ensure no ungrouped files or directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.14	Ensure all public directories are owned by root or a system account	<input type="checkbox"/>	<input type="checkbox"/>
6.1.15	Audit SUID executables	<input type="checkbox"/>	<input type="checkbox"/>
6.1.16	Audit SGID executables	<input type="checkbox"/>	<input type="checkbox"/>
6.1.17	Ensure the "/var/log/messages" file has mode "0640" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.18	Ensure the "/var/log/messages" file is owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.19	Ensure the "/var/log/messages" file is group-owned by root	<input type="checkbox"/>	<input type="checkbox"/>

6.1.20	Ensure the "/var/log" directory has a mode of "0755" or less	<input type="checkbox"/>	<input type="checkbox"/>
6.1.21	Ensure the "/var/log" directory is owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.22	Ensure the "/var/log" directory is group-owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.23	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories have mode "0755" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.24	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.25	Ensure the system commands contained in "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.26	Ensure the system-wide shared library files contained in the "/lib, /lib64, /usr/lib, /usr/lib64" directories have mode "0755" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.27	Ensure the system-wide shared library files are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.28	Ensure the system-wide shared library files are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.29	Ensure world-writable directories are owned by root, sys, bin, or an application user	<input type="checkbox"/>	<input type="checkbox"/>
6.1.30	Ensure world-writable directories are group-owned by root, sys, bin, or an application group	<input type="checkbox"/>	<input type="checkbox"/>
6.1.31	Ensure local initialization files do not execute world-writable programs	<input type="checkbox"/>	<input type="checkbox"/>
6.1.32	Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer	<input type="checkbox"/>	<input type="checkbox"/>
6.1.33	Ensure the operating system prevents users from disabling the tmux terminal multiplexer	<input type="checkbox"/>	<input type="checkbox"/>
6.1.34	Ensure the operating system enables a user's session lock until that user re-establishes access	<input type="checkbox"/>	<input type="checkbox"/>
6.1.35	Ensure the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
6.1.36	Ensure the operating system initiates a session lock after 15 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
6.1.37	Ensure all accounts on the system are assigned to an active system, application, or user account	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1	Ensure password fields are not empty	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Ensure root PATH Integrity	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Ensure no legacy "+" entries exist in /etc/shadow	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure no legacy "+" entries exist in /etc/group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure root is the only UID 0 account	<input type="checkbox"/>	<input type="checkbox"/>

6.2.7	Ensure users' home directories permissions are 750 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
6.2.9	Ensure users own their home directories	<input type="checkbox"/>	<input type="checkbox"/>
6.2.10	Ensure users' dot files are not group or world writable	<input type="checkbox"/>	<input type="checkbox"/>
6.2.11	Ensure no users have .forward files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.12	Ensure no users have .netrc files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.13	Ensure users' .netrc Files are not group or world accessible	<input type="checkbox"/>	<input type="checkbox"/>
6.2.14	Ensure no users have .rhosts files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.20	Ensure shadow group is empty	<input type="checkbox"/>	<input type="checkbox"/>
6.2.21	Ensure all users' home directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.22	Ensure the assigned home directory of all local interactive users is group-owned by that user's primary GID	<input type="checkbox"/>	<input type="checkbox"/>
6.2.23	Ensure the assigned home directory of all local interactive users exists	<input type="checkbox"/>	<input type="checkbox"/>
6.2.24	Ensure all local interactive users are assigned a home directory upon creation	<input type="checkbox"/>	<input type="checkbox"/>
6.2.25	Ensure all local initialization files have a mode of "0740" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.2.26	Ensure all local files and directories have a valid owner	<input type="checkbox"/>	<input type="checkbox"/>
6.2.27	Ensure all local files and directories have a valid group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.28	Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file	<input type="checkbox"/>	<input type="checkbox"/>
6.2.29	Ensure file executable search path statements do not share sensitive home directory information	<input type="checkbox"/>	<input type="checkbox"/>
6.2.30	Ensure local interactive users have a home directory assigned	<input type="checkbox"/>	<input type="checkbox"/>
6.2.31	Ensure the operating system limits the number of concurrent sessions to "10" for all accounts and/or account types	<input type="checkbox"/>	<input type="checkbox"/>
6.2.32	Ensure the operating system enables a user's session lock until that user re-establishes access	<input type="checkbox"/>	<input type="checkbox"/>
6.2.33	Ensure the operating system enables the user to initiate a session lock	<input type="checkbox"/>	<input type="checkbox"/>
6.2.34	Ensure the operating system prevents a user from overriding settings for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
6.2.35	Ensure all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750"	<input type="checkbox"/>	<input type="checkbox"/>
6.2.36	Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of	<input type="checkbox"/>	<input type="checkbox"/>
6.2.37	Ensure temporary accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>

6.3	Ensure the operating system removes all software components after updated versions have been installed	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure there are no ".shosts" files on the operating system	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Ensure there are no "shosts.equiv" files on the operating system	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of cramfs filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure mounting of vFAT filesystems is limited	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure mounting of squashfs filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure mounting of udf filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Ensure /tmp is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Ensure nodev option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Ensure nosuid option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Ensure noexec option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	Ensure separate partition exists for /var	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Ensure separate partition exists for /var/tmp	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Ensure nodev option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Ensure nosuid option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Ensure noexec option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.11	Ensure separate partition exists for /var/log	<input type="checkbox"/>	<input type="checkbox"/>
1.1.13	Ensure separate partition exists for /home	<input type="checkbox"/>	<input type="checkbox"/>
1.1.14	Ensure nodev option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.15	Ensure nodev option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.16	Ensure nosuid option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.17	Ensure noexec option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.18	Ensure nodev option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.19	Ensure nosuid option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.20	Ensure noexec option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.21	Ensure sticky bit is set on all world-writable directories	<input type="checkbox"/>	<input type="checkbox"/>
1.1.22	Disable Automounting	<input type="checkbox"/>	<input type="checkbox"/>
1.1.23	Disable USB Storage	<input type="checkbox"/>	<input type="checkbox"/>
1.1.24	Ensure file systems that contain user home directories are mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.25	Ensure the "/boot" directory is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.26	Ensure all non-root local partitions are mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.27	Ensure file systems that are being NFS-imported are mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.29	Ensure file systems being imported via NFS are mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.30	Ensure a separate file system/partition has been created for non-privileged local interactive user home directories	<input type="checkbox"/>	<input type="checkbox"/>

1.1.31	Ensure "/var/log" is mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.32	Ensure "/var/log" is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.33	Ensure "/var/log" is mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.34	Ensure "/var/log/audit" is mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.35	Ensure "/var/log/audit" is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.36	Ensure "/var/log/audit" is mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.37	Ensure the "/boot/efi" directory is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.38	Ensure file systems that contain user home directories are mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1	Ensure GPG keys are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Ensure gpgcheck is globally activated	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Ensure package manager repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Ensure DNF is configured to perform a signature check on local packages	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Ensure sudo is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Ensure the "/etc/sudoers" file has no occurrences of "NOPASSWD"	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	Ensure the "/etc/sudoers" file has no occurrences of "!authenticate"	<input type="checkbox"/>	<input type="checkbox"/>
1.3.6	Ensure the "sudoers" file restricts sudo access to authorized personnel	<input type="checkbox"/>	<input type="checkbox"/>
1.3.7	Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation	<input type="checkbox"/>	<input type="checkbox"/>
1.3.8	Ensure the operating system requires re-authentication when using the "sudo" command to elevate privileges	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure permissions on bootloader config are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure bootloader password is set	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Ensure authentication required for single user mode	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Ensure the encrypted grub superusers password is set for systems booted with UEFI	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Ensure the encrypted grub superusers password is set for system booted with BIOS	<input type="checkbox"/>	<input type="checkbox"/>
1.5.6	Ensure the operating system requires authentication for rescue mode	<input type="checkbox"/>	<input type="checkbox"/>
1.5.7	Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities	<input type="checkbox"/>	<input type="checkbox"/>
1.5.8	Ensure GRUB 2 is configured to disable vsyscalls	<input type="checkbox"/>	<input type="checkbox"/>
1.5.9	Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities	<input type="checkbox"/>	<input type="checkbox"/>

1.5.10	Ensure the operating system is configured to boot to the command line	<input type="checkbox"/>	<input type="checkbox"/>
1.5.11	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed	<input type="checkbox"/>	<input type="checkbox"/>
1.5.12	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds	<input type="checkbox"/>	<input type="checkbox"/>
1.5.13	Ensure a unique name is set as the "superusers" account (UEFI)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.14	Ensure a unique name is set as the "superusers" account (BIOS)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.15	Ensure the operating system requires authentication upon booting into emergency mode	<input type="checkbox"/>	<input type="checkbox"/>
1.6.1	Ensure core dumps are restricted	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure the operating system is not configured to acquire, save, or process core dumps	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure kernel core dumps are disabled unless needed	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure the operating system disables core dumps for all users	<input type="checkbox"/>	<input type="checkbox"/>
1.6.7	Ensure the operating system disables storing core dumps for all users	<input type="checkbox"/>	<input type="checkbox"/>
1.6.8	Ensure the operating system disables core dump backtraces	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.1	Ensure SELinux is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.2	Ensure SELinux is not disabled in bootloader configuration	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.3	Ensure SELinux policy is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.4	Ensure the SELinux state is enforcing	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.5	Ensure no unconfined services exist	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.8	Ensure the operating system has the policycoreutils package installed	<input type="checkbox"/>	<input type="checkbox"/>
1.8.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.8.2	Ensure message of the day is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.3	Ensure local login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.4	Ensure remote login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.5	Ensure permissions on /etc/motd are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.6	Ensure permissions on /etc/issue are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.7	Ensure permissions on /etc/issue.net are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.8	Ensure the Standard Mandatory DoD Notice and Consent Banner is displayed before granting access to the system via SSH logon	<input type="checkbox"/>	<input type="checkbox"/>
1.8.9	Ensure the operating system displays a banner before granting access to the operating system via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>

1.9.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.3	Ensure GDM login banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.9.4	Ensure last logged in user display is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.9.6	Ensure a Standard Mandatory DoD Notice and Consent Banner is displayed via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.7	Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.8	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.9	Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated	<input type="checkbox"/>	<input type="checkbox"/>
1.9.10	Ensure the operating system disables the user logon list for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
1.9.11	Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.12	Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.10	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
1.13	Ensure the operating system implements DoD-approved encryption	<input type="checkbox"/>	<input type="checkbox"/>
1.14	Ensure the operating system prevents unauthorized modification of all information at rest by using disk encryption	<input type="checkbox"/>	<input type="checkbox"/>
1.15	Ensure kernel image loading is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure the operating system is configured to enable DAC on symlinks	<input type="checkbox"/>	<input type="checkbox"/>
1.17	Ensure the operating system is configured to enable DAC on hardlinks	<input type="checkbox"/>	<input type="checkbox"/>
1.18	Ensure the operating system is configured to restrict access to the kernel message buffer	<input type="checkbox"/>	<input type="checkbox"/>
1.19	Ensure the operating system is configured to prevent kernel profiling by unprivileged users	<input type="checkbox"/>	<input type="checkbox"/>
1.20	Ensure the operating system has the packages required for multifactor authentication	<input type="checkbox"/>	<input type="checkbox"/>
1.21	Ensure the operating system implements certificate status checking for multifactor authentication	<input type="checkbox"/>	<input type="checkbox"/>
1.22	Ensure the operating system accepts PIV credentials	<input type="checkbox"/>	<input type="checkbox"/>
1.24	Ensure kernel page-table isolation is enabled	<input type="checkbox"/>	<input type="checkbox"/>

1.25	Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall	<input type="checkbox"/>	<input type="checkbox"/>
1.26	Ensure the operating system restricts usage of ptrace to descendant processes	<input type="checkbox"/>	<input type="checkbox"/>
1.27	Ensure the operating system restricts exposed kernel pointer addresses access	<input type="checkbox"/>	<input type="checkbox"/>
1.30	Ensure the operating system disables the use of user namespaces	<input type="checkbox"/>	<input type="checkbox"/>
1.31	Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service	<input type="checkbox"/>	<input type="checkbox"/>
1.32	Ensure the "tmux" package installed	<input type="checkbox"/>	<input type="checkbox"/>
1.33	Ensure the operating system enables hardening for the BPF JIT	<input type="checkbox"/>	<input type="checkbox"/>
2.2.20	Ensure the operating system has enabled the hardware random number generator entropy gatherer service	<input type="checkbox"/>	<input type="checkbox"/>
2.2.28	Ensure the TFTP daemon is configured to operate in secure mode	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure IP forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure the system does not accept router advertisements on IPv6 interfaces, unless the system is a router	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure the system does not accept router advertisements on IPv6 interfaces by default, unless the system is a router	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure Reverse Path Filtering is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.8	Ensure TCP SYN Cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.9	Ensure IPv6 router advertisements are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.10	Ensure the operating system does not accept IPv6 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.11	Ensure the operating system does not accept IPv6 source-routed packets	<input type="checkbox"/>	<input type="checkbox"/>
3.2.12	Ensure the operating system does not accept IPv6 source-routed packets by default	<input type="checkbox"/>	<input type="checkbox"/>
3.2.13	Ensure the operating system ignores IPv6 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.14	Ensure network interfaces are not in promiscuous mode	<input type="checkbox"/>	<input type="checkbox"/>
3.2.15	Ensure the operating system does not accept IPv4 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.16	Ensure the operating system does not accept IPv4 source-routed packet	<input type="checkbox"/>	<input type="checkbox"/>

3.2.17	Ensure the operating system does not accept IPv4 source-routed packets by default	<input type="checkbox"/>	<input type="checkbox"/>
3.2.18	Ensure the operating system ignores IPv4 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.1	Ensure a Firewall package is installed	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.1	Ensure firewalld service is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure iptables service is not enabled with firewalld	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.3	Ensure nftables is not enabled with firewalld	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.4	Ensure firewalld default zone is set	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.5	Ensure network interfaces are assigned to appropriate zone	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.6	Ensure firewalld drops unnecessary services and ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.7	Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.8	Ensure "firewalld" is installed	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.1	Ensure iptables are flushed with nftables	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.2	Ensure an nftables table exists	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.3	Ensure nftables base chains exist	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.4	Ensure nftables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.5	Ensure nftables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.6	Ensure nftables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.7	Ensure nftables service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.8	Ensure nftables rules are permanent	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.9	Ensure "nftables" is configured to allow rate limits on any connection to the system	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.1	Ensure iptables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.2	Ensure iptables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.3	Ensure iptables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.4	Ensure iptables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.5	Ensure iptables is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.1	Ensure ip6tables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.2	Ensure ip6tables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.3	Ensure ip6tables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.4	Ensure ip6tables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.5	Ensure ip6tables is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure at least two name servers are configured if using DNS resolution	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Ensure auditd is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Ensure auditd service is enabled	<input type="checkbox"/>	<input type="checkbox"/>

4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	Ensure audit_backlog_limit is sufficient	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.5	Ensure the audit service is configured to produce audit records	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.3	Ensure system is disabled when audit logs are full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure the SA and ISSO are notified in the event of an audit processing failure	<input type="checkbox"/>	<input type="checkbox"/>
4.1.19	Ensure the audit system prevents unauthorized changes	<input type="checkbox"/>	<input type="checkbox"/>
4.1.41	Ensure the operating system's audit logs have a mode of "0600" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
4.1.42	Ensure the operating system's audit logs are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.43	Ensure the audit logs are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.44	Ensure the audit log directory is owned by "root" to prevent unauthorized read access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.45	Ensure the audit log directory is group-owned by "root" to prevent unauthorized read access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.46	Ensure the audit log directories have a mode of "0700" or less permissive by first determining where the audit logs are stored	<input type="checkbox"/>	<input type="checkbox"/>
4.1.101	Ensure the files in directory "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
4.1.102	Ensure the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode	<input type="checkbox"/>	<input type="checkbox"/>
4.1.103	Ensure the audit tools are owned by "root" to prevent any unauthorized access, deletion, or modification	<input type="checkbox"/>	<input type="checkbox"/>
4.1.104	Ensure the audit tools are group-owned by "root" to prevent any unauthorized access, deletion, or modification	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.1	Ensure rsyslog is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.3	Ensure the operating system monitors all remote access methods	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.4	Ensure rsyslog Service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.5	Ensure rsyslog default file permissions configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.6	Ensure logging is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.8	Ensure remote rsyslog messages are only accepted on designated log hosts.	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure permissions on all logfiles are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure administrators are notified if an audit processing failure occurs by modifying "/etc/aliases"	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure cron daemon is enabled	<input type="checkbox"/>	<input type="checkbox"/>

5.1.2	Ensure permissions on /etc/crontab are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on /etc/cron.hourly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure permissions on /etc/cron.daily are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure permissions on /etc/cron.weekly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure permissions on /etc/cron.monthly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure permissions on /etc/cron.d are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.8	Ensure at/cron is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure SSH private key files have a passcode	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure SSH access is limited	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure permissions on SSH private host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure permissions on SSH public host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure SSH LogLevel is appropriate	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	Ensure SSH IgnoreRhosts is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	Ensure SSH HostbasedAuthentication is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	Ensure SSH root login is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	Ensure SSH PermitEmptyPasswords is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.2.14	Ensure SSH PermitUserEnvironment is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.15	Ensure SSH Idle Timeout Interval is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.16	Ensure SSH LoginGraceTime is set to one minute or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.17	Ensure SSH warning banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.18	Ensure SSH PAM is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.19	Ensure SSH AllowTcpForwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.20	Ensure SSH MaxStartups is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.21	Ensure SSH MaxSessions is set to 4 or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.22	Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>
5.2.24	Ensure the SSH server uses strong entropy	<input type="checkbox"/>	<input type="checkbox"/>
5.2.26	Ensure the SSH daemon performs strict mode checking of home directory configuration files	<input type="checkbox"/>	<input type="checkbox"/>
5.2.27	Ensure the SSH daemon performs compression after a user successfully authenticates	<input type="checkbox"/>	<input type="checkbox"/>
5.2.28	Ensure the SSH daemon does not allow authentication using known host's authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.29	Ensure the SSH daemon does not allow Kerberos authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.30	Ensure null passwords cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.2.31	Ensure SSH provides users with feedback on when account accesses last occurred	<input type="checkbox"/>	<input type="checkbox"/>

5.2.33	Ensure the SSH server is configured to force frequent session key renegotiation	<input type="checkbox"/>	<input type="checkbox"/>
5.2.34	Ensure the SSH daemon prevents remote hosts from connecting to the proxy display	<input type="checkbox"/>	<input type="checkbox"/>
5.2.36	Ensure the SSH daemon does not allow GSSAPI authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.38	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	Create custom authselect profile	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2	Select authselect profile	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	Ensure authselect includes with-faillock	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1	Ensure password creation requirements are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2	Ensure the system locks an account after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3	Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts within 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.4	Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.5	Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.6	Ensure lockout for failed password attempts is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.7	Ensure password reuse is limited	<input type="checkbox"/>	<input type="checkbox"/>
5.4.9	Ensure a minimum number of hash rounds is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.10	Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes until released by an administrator	<input type="checkbox"/>	<input type="checkbox"/>
5.4.11	Ensure the "/etc/security/faillock.conf" file is configured to lock an account until released by an administrator after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.12	Ensure the faillock directory contents persist after a reboot	<input type="checkbox"/>	<input type="checkbox"/>
5.4.13	Ensure the "/etc/security/faillock.conf" file is configured to use a non-default faillock directory to ensure contents persist after reboot	<input type="checkbox"/>	<input type="checkbox"/>
5.4.14	Ensure the system prevents informative messages to the user about logon information	<input type="checkbox"/>	<input type="checkbox"/>
5.4.15	Ensure the "/etc/security/faillock.conf" file is configured to prevent informative messages about logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.18	Ensure the system includes the root account when locking an account after three unsuccessful logon attempts within a period of 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.20	Ensure the operating system prohibits password reuse for a minimum of five generations	<input type="checkbox"/>	<input type="checkbox"/>

5.4.21	Ensure the operating system uses multifactor authentication for local access to accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.22	Ensure the date and time of the last successful account logon upon logon is displayed	<input type="checkbox"/>	<input type="checkbox"/>
5.4.24	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/system-auth" file	<input type="checkbox"/>	<input type="checkbox"/>
5.4.25	Ensure blank or null passwords in the "system-auth" file cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.4.26	Ensure blank or null passwords in the "password-auth" file cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.4.27	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/password-auth" file	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.1	Ensure password expiration is 365 days or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.3	Ensure the value of the "maxrepeat" option in "/etc/security/pwquality.conf" is "3"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.4	Ensure the value of the "difok" option in "/etc/security/pwquality.conf" is "8"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.5	Ensure the value of the "minclass" option in "/etc/security/pwquality.conf" is "4"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.6	Ensure the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" is "4"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.7	Ensure the value for "dcredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.8	Ensure the value for "lcredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.9	Ensure the value for "ucredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.10	Ensure the operating system uses "pwquality" to enforce the password complexity rules	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.11	Ensure minimum days between password changes is 7 or more	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.12	Ensure password expiration warning days is 7 or more	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.13	Ensure inactive password lock is 30 days or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.14	Ensure all users last password change date is in the past	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.15	Ensure the minimum time period between password changes for each user account is one day or greater	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.16	Ensure the operating system enforces 24 hours/1 day as the minimum password lifetime for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.17	Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.18	Ensure the maximum time period for existing passwords is restricted to 60 days	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.19	Ensure the operating system enforces a minimum 15-character password length	<input type="checkbox"/>	<input type="checkbox"/>

5.5.1.20	Ensure the operating system enforces a minimum 15-character password length for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.21	Ensure the value for "ocredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.22	Ensure the operating system prevents the use of dictionary words for passwords	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.23	Ensure the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt	<input type="checkbox"/>	<input type="checkbox"/>
5.5.2	Ensure system accounts are secured	<input type="checkbox"/>	<input type="checkbox"/>
5.5.3	Ensure default user shell timeout is 900 seconds or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.5	Ensure default group for the root account is GID 0	<input type="checkbox"/>	<input type="checkbox"/>
5.5.6	Ensure default user umask is 027 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
5.5.7	Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.5.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
5.5.9	Ensure the default umask for all local interactive users is "077"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.10	Ensure the umask default for installed shells is "077"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.11	Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files	<input type="checkbox"/>	<input type="checkbox"/>
5.6	Ensure root login is restricted to system console	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure PKI-based authentication has valid certificates	<input type="checkbox"/>	<input type="checkbox"/>
5.8	Ensure access to the su command is restricted	<input type="checkbox"/>	<input type="checkbox"/>
5.9	Ensure the operating system prevents system daemons from using Kerberos for authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.11	Ensure SSSD prohibits the use of cached authentications after one day	<input type="checkbox"/>	<input type="checkbox"/>
5.12	Ensure "fapolicyd" is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.13	Ensure USBGuard has a policy configured	<input type="checkbox"/>	<input type="checkbox"/>
5.19	Ensure USBGuard is installed on the operating system	<input type="checkbox"/>	<input type="checkbox"/>
5.20	Ensure the operating system has enabled the use of the USBGuard	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Audit system file permissions	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure permissions on /etc/passwd are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Ensure permissions on /etc/passwd- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.4	Ensure permissions on /etc/shadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.5	Ensure permissions on /etc/shadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.6	Ensure permissions on /etc/gshadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.7	Ensure permissions on /etc/gshadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.8	Ensure permissions on /etc/group are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.9	Ensure permissions on /etc/group- are configured	<input type="checkbox"/>	<input type="checkbox"/>

6.1.10	Ensure the root account is the only account that has unrestricted access to the operating system	<input type="checkbox"/>	<input type="checkbox"/>
6.1.11	Ensure no world writable files exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.12	Ensure no unowned files or directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.13	Ensure no ungrouped files or directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.14	Ensure all public directories are owned by root or a system account	<input type="checkbox"/>	<input type="checkbox"/>
6.1.15	Audit SUID executables	<input type="checkbox"/>	<input type="checkbox"/>
6.1.16	Audit SGID executables	<input type="checkbox"/>	<input type="checkbox"/>
6.1.17	Ensure the "/var/log/messages" file has mode "0640" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.18	Ensure the "/var/log/messages" file is owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.19	Ensure the "/var/log/messages" file is group-owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.20	Ensure the "/var/log" directory has a mode of "0755" or less	<input type="checkbox"/>	<input type="checkbox"/>
6.1.21	Ensure the "/var/log" directory is owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.22	Ensure the "/var/log" directory is group-owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.23	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories have mode "0755" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.24	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.25	Ensure the system commands contained in "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.26	Ensure the system-wide shared library files contained in the "/lib, /lib64, /usr/lib, /usr/lib64" directories have mode "0755" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.27	Ensure the system-wide shared library files are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.28	Ensure the system-wide shared library files are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.29	Ensure world-writable directories are owned by root, sys, bin, or an application user	<input type="checkbox"/>	<input type="checkbox"/>
6.1.30	Ensure world-writable directories are group-owned by root, sys, bin, or an application group	<input type="checkbox"/>	<input type="checkbox"/>
6.1.31	Ensure local initialization files do not execute world-writable programs	<input type="checkbox"/>	<input type="checkbox"/>
6.1.32	Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer	<input type="checkbox"/>	<input type="checkbox"/>
6.1.33	Ensure the operating system prevents users from disabling the tmux terminal multiplexer	<input type="checkbox"/>	<input type="checkbox"/>
6.1.34	Ensure the operating system enables a user's session lock until that user re-establishes access	<input type="checkbox"/>	<input type="checkbox"/>

6.1.35	Ensure the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
6.1.36	Ensure the operating system initiates a session lock after 15 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
6.1.37	Ensure all accounts on the system are assigned to an active system, application, or user account	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1	Ensure password fields are not empty	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Ensure root PATH Integrity	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Ensure no legacy "+" entries exist in /etc/shadow	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure no legacy "+" entries exist in /etc/group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure root is the only UID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure users' home directories permissions are 750 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
6.2.9	Ensure users own their home directories	<input type="checkbox"/>	<input type="checkbox"/>
6.2.10	Ensure users' dot files are not group or world writable	<input type="checkbox"/>	<input type="checkbox"/>
6.2.11	Ensure no users have .forward files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.12	Ensure no users have .netrc files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.13	Ensure users' .netrc Files are not group or world accessible	<input type="checkbox"/>	<input type="checkbox"/>
6.2.14	Ensure no users have .rhosts files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.15	Ensure all groups in /etc/passwd exist in /etc/group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.16	Ensure no duplicate UIDs exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.17	Ensure no duplicate GIDs exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.18	Ensure no duplicate user names exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.19	Ensure no duplicate group names exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.20	Ensure shadow group is empty	<input type="checkbox"/>	<input type="checkbox"/>
6.2.21	Ensure all users' home directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.22	Ensure the assigned home directory of all local interactive users is group-owned by that user's primary GID	<input type="checkbox"/>	<input type="checkbox"/>
6.2.23	Ensure the assigned home directory of all local interactive users exists	<input type="checkbox"/>	<input type="checkbox"/>
6.2.24	Ensure all local interactive users are assigned a home directory upon creation	<input type="checkbox"/>	<input type="checkbox"/>
6.2.25	Ensure all local initialization files have a mode of "0740" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.2.26	Ensure all local files and directories have a valid owner	<input type="checkbox"/>	<input type="checkbox"/>
6.2.27	Ensure all local files and directories have a valid group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.28	Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file	<input type="checkbox"/>	<input type="checkbox"/>
6.2.29	Ensure file executable search path statements do not share sensitive home directory information	<input type="checkbox"/>	<input type="checkbox"/>
6.2.30	Ensure local interactive users have a home directory assigned	<input type="checkbox"/>	<input type="checkbox"/>

6.2.31	Ensure the operating system limits the number of concurrent sessions to "10" for all accounts and/or account types	<input type="checkbox"/>	<input type="checkbox"/>
6.2.32	Ensure the operating system enables a user's session lock until that user re-establishes access	<input type="checkbox"/>	<input type="checkbox"/>
6.2.33	Ensure the operating system enables the user to initiate a session lock	<input type="checkbox"/>	<input type="checkbox"/>
6.2.34	Ensure the operating system prevents a user from overriding settings for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
6.2.35	Ensure all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750"	<input type="checkbox"/>	<input type="checkbox"/>
6.2.36	Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of	<input type="checkbox"/>	<input type="checkbox"/>
6.2.37	Ensure temporary accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure the operating system removes all software components after updated versions have been installed	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure there are no ".shosts" files on the operating system	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Ensure there are no "shosts.equiv" files on the operating system	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of cramfs filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure mounting of vFAT filesystems is limited	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure mounting of squashfs filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure mounting of udf filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Ensure /tmp is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Ensure nodev option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Ensure nosuid option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Ensure noexec option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	Ensure separate partition exists for /var	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Ensure separate partition exists for /var/tmp	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Ensure nodev option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Ensure nosuid option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Ensure noexec option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.11	Ensure separate partition exists for /var/log	<input type="checkbox"/>	<input type="checkbox"/>
1.1.12	Ensure separate partition exists for /var/log/audit	<input type="checkbox"/>	<input type="checkbox"/>
1.1.13	Ensure separate partition exists for /home	<input type="checkbox"/>	<input type="checkbox"/>
1.1.14	Ensure nodev option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.15	Ensure nodev option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.16	Ensure nosuid option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.17	Ensure noexec option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.18	Ensure nodev option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.19	Ensure nosuid option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.20	Ensure noexec option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.21	Ensure sticky bit is set on all world-writable directories	<input type="checkbox"/>	<input type="checkbox"/>
1.1.22	Disable Automounting	<input type="checkbox"/>	<input type="checkbox"/>
1.1.23	Disable USB Storage	<input type="checkbox"/>	<input type="checkbox"/>
1.1.24	Ensure file systems that contain user home directories are mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.25	Ensure the "/boot" directory is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.26	Ensure all non-root local partitions are mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.27	Ensure file systems that are being NFS-imported are mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.29	Ensure file systems being imported via NFS are mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>

1.1.30	Ensure a separate file system/partition has been created for non-privileged local interactive user home directories	<input type="checkbox"/>	<input type="checkbox"/>
1.1.31	Ensure "/var/log" is mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.32	Ensure "/var/log" is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.33	Ensure "/var/log" is mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.34	Ensure "/var/log/audit" is mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.35	Ensure "/var/log/audit" is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.36	Ensure "/var/log/audit" is mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.37	Ensure the "/boot/efi" directory is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.38	Ensure file systems that contain user home directories are mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1	Ensure GPG keys are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Ensure gpgcheck is globally activated	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Ensure package manager repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Ensure DNF is configured to perform a signature check on local packages	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Ensure sudo is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
1.3.3	Ensure sudo log file exists	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Ensure the "/etc/sudoers" file has no occurrences of "NOPASSWD"	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	Ensure the "/etc/sudoers" file has no occurrences of "!authenticate"	<input type="checkbox"/>	<input type="checkbox"/>
1.3.6	Ensure the "sudoers" file restricts sudo access to authorized personnel	<input type="checkbox"/>	<input type="checkbox"/>
1.3.7	Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation	<input type="checkbox"/>	<input type="checkbox"/>
1.3.8	Ensure the operating system requires re-authentication when using the "sudo" command to elevate privileges	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure permissions on bootloader config are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure bootloader password is set	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Ensure authentication required for single user mode	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Ensure the encrypted grub superusers password is set for systems booted with UEFI	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Ensure the encrypted grub superusers password is set for system booted with BIOS	<input type="checkbox"/>	<input type="checkbox"/>
1.5.6	Ensure the operating system requires authentication for rescue mode	<input type="checkbox"/>	<input type="checkbox"/>
1.5.7	Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities	<input type="checkbox"/>	<input type="checkbox"/>
1.5.8	Ensure GRUB 2 is configured to disable vsyscalls	<input type="checkbox"/>	<input type="checkbox"/>

1.5.9	Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities	<input type="checkbox"/>	<input type="checkbox"/>
1.5.10	Ensure the operating system is configured to boot to the command line	<input type="checkbox"/>	<input type="checkbox"/>
1.5.11	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed	<input type="checkbox"/>	<input type="checkbox"/>
1.5.12	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds	<input type="checkbox"/>	<input type="checkbox"/>
1.5.13	Ensure a unique name is set as the "superusers" account (UEFI)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.14	Ensure a unique name is set as the "superusers" account (BIOS)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.15	Ensure the operating system requires authentication upon booting into emergency mode	<input type="checkbox"/>	<input type="checkbox"/>
1.6.1	Ensure core dumps are restricted	<input type="checkbox"/>	<input type="checkbox"/>
1.6.2	Ensure address space layout randomization (ASLR) is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure the operating system is not configured to acquire, save, or process core dumps	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure kernel core dumps are disabled unless needed	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure the operating system disables core dumps for all users	<input type="checkbox"/>	<input type="checkbox"/>
1.6.7	Ensure the operating system disables storing core dumps for all users	<input type="checkbox"/>	<input type="checkbox"/>
1.6.8	Ensure the operating system disables core dump backtraces	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.1	Ensure SELinux is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.2	Ensure SELinux is not disabled in bootloader configuration	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.3	Ensure SELinux policy is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.4	Ensure the SELinux state is enforcing	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.5	Ensure no unconfined services exist	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.6	Ensure SETroubleshoot is not installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.7	Ensure the MCS Translation Service (mcstrans) is not installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.8	Ensure the operating system has the policycoreutils package installed	<input type="checkbox"/>	<input type="checkbox"/>
1.8.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.8.2	Ensure message of the day is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.3	Ensure local login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.4	Ensure remote login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.5	Ensure permissions on /etc/motd are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.6	Ensure permissions on /etc/issue are configured	<input type="checkbox"/>	<input type="checkbox"/>

1.8.7	Ensure permissions on /etc/issue.net are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.8	Ensure the Standard Mandatory DoD Notice and Consent Banner is displayed before granting access to the system via SSH logon	<input type="checkbox"/>	<input type="checkbox"/>
1.8.9	Ensure the operating system displays a banner before granting access to the operating system via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.2	Ensure GNOME Display Manager is removed	<input type="checkbox"/>	<input type="checkbox"/>
1.9.3	Ensure GDM login banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.9.4	Ensure last logged in user display is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.9.5	Ensure XDCMP is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.9.6	Ensure a Standard Mandatory DoD Notice and Consent Banner is displayed via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.7	Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.8	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.9	Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated	<input type="checkbox"/>	<input type="checkbox"/>
1.9.10	Ensure the operating system disables the user logon list for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
1.9.11	Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.12	Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.10	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure system-wide crypto policy is not legacy	<input type="checkbox"/>	<input type="checkbox"/>
1.12	Ensure system-wide crypto policy is FUTURE or FIPS	<input type="checkbox"/>	<input type="checkbox"/>
1.13	Ensure the operating system implements DoD-approved encryption	<input type="checkbox"/>	<input type="checkbox"/>
1.14	Ensure the operating system prevents unauthorized modification of all information at rest by using disk encryption	<input type="checkbox"/>	<input type="checkbox"/>
1.15	Ensure kernel image loading is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure the operating system is configured to enable DAC on symlinks	<input type="checkbox"/>	<input type="checkbox"/>
1.17	Ensure the operating system is configured to enable DAC on hardlinks	<input type="checkbox"/>	<input type="checkbox"/>

1.18	Ensure the operating system is configured to restrict access to the kernel message buffer	<input type="checkbox"/>	<input type="checkbox"/>
1.19	Ensure the operating system is configured to prevent kernel profiling by unprivileged users	<input type="checkbox"/>	<input type="checkbox"/>
1.20	Ensure the operating system has the packages required for multifactor authentication	<input type="checkbox"/>	<input type="checkbox"/>
1.21	Ensure the operating system implements certificate status checking for multifactor authentication	<input type="checkbox"/>	<input type="checkbox"/>
1.22	Ensure the operating system accepts PIV credentials	<input type="checkbox"/>	<input type="checkbox"/>
1.23	Ensure the NX (no-execution) bit flag is set on the system	<input type="checkbox"/>	<input type="checkbox"/>
1.24	Ensure kernel page-table isolation is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.25	Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall	<input type="checkbox"/>	<input type="checkbox"/>
1.26	Ensure the operating system restricts usage of ptrace to descendant processes	<input type="checkbox"/>	<input type="checkbox"/>
1.27	Ensure the operating system restricts exposed kernel pointer addresses access	<input type="checkbox"/>	<input type="checkbox"/>
1.28	Ensure the operating system disables the ability to load the firewire-core kernel module	<input type="checkbox"/>	<input type="checkbox"/>
1.29	Ensure the operating system disables the ability to load the USB Storage kernel module	<input type="checkbox"/>	<input type="checkbox"/>
1.30	Ensure the operating system disables the use of user namespaces	<input type="checkbox"/>	<input type="checkbox"/>
1.31	Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service	<input type="checkbox"/>	<input type="checkbox"/>
1.32	Ensure the "tmux" package installed	<input type="checkbox"/>	<input type="checkbox"/>
1.33	Ensure the operating system enables hardening for the BPF JIT	<input type="checkbox"/>	<input type="checkbox"/>
1.34	Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	Ensure xinetd is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.1	Ensure time synchronization is in use	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.2	Ensure chrony is configured	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.3	Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.4	Ensure the operating system disables the chrony daemon from acting as a server	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.5	Ensure the operating system disables network management of the chrony daemon	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure X Window System is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure rsync service is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure Avahi Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure SNMP Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>

2.2.6	Ensure HTTP Proxy Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Ensure Samba is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Ensure IMAP and POP3 server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	Ensure HTTP server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	Ensure FTP Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure DNS Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.12	Ensure NFS is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure RPC is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	Ensure LDAP server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	Ensure DHCP Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	Ensure the telnet-server package is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.17	Ensure CUPS is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.18	Ensure NIS Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.19	Ensure mail transfer agent is configured for local-only mode	<input type="checkbox"/>	<input type="checkbox"/>
2.2.20	Ensure the operating system has enabled the hardware random number generator entropy gatherer service	<input type="checkbox"/>	<input type="checkbox"/>
2.2.21	Ensure automated bug reporting tools are not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.22	Ensure the sendmail package is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.23	Ensure the rsh-server package is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.24	Ensure a camera is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.25	Ensure the operating system is configured to mask the debug-shell systemd service	<input type="checkbox"/>	<input type="checkbox"/>
2.2.26	Ensure a TFTP server has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.27	Ensure the operating system is configured to prevent unrestricted mail relaying	<input type="checkbox"/>	<input type="checkbox"/>
2.2.28	Ensure the TFTP daemon is configured to operate in secure mode	<input type="checkbox"/>	<input type="checkbox"/>
2.2.29	Ensure an FTP server has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.30	Ensure the gssproxy package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.31	Ensure the iputils package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.32	Ensure the tuned package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.33	Ensure the krb5-server package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure NIS Client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure telnet client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure LDAP client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure IP forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure the system does not accept router advertisements on IPv6 interfaces, unless the system is a router	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure the system does not accept router advertisements on IPv6 interfaces by default, unless the system is a router	<input type="checkbox"/>	<input type="checkbox"/>

3.2.1	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure Reverse Path Filtering is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.8	Ensure TCP SYN Cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.9	Ensure IPv6 router advertisements are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.10	Ensure the operating system does not accept IPv6 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.11	Ensure the operating system does not accept IPv6 source-routed packets	<input type="checkbox"/>	<input type="checkbox"/>
3.2.12	Ensure the operating system does not accept IPv6 source-routed packets by default	<input type="checkbox"/>	<input type="checkbox"/>
3.2.13	Ensure the operating system ignores IPv6 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.14	Ensure network interfaces are not in promiscuous mode	<input type="checkbox"/>	<input type="checkbox"/>
3.2.15	Ensure the operating system does not accept IPv4 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.16	Ensure the operating system does not accept IPv4 source-routed packet	<input type="checkbox"/>	<input type="checkbox"/>
3.2.17	Ensure the operating system does not accept IPv4 source-routed packets by default	<input type="checkbox"/>	<input type="checkbox"/>
3.2.18	Ensure the operating system ignores IPv4 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure DCCP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure SCTP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure RDS is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure TIPC is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure ATM is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure CAN is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.1	Ensure a Firewall package is installed	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.1	Ensure firewalld service is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure iptables service is not enabled with firewalld	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.3	Ensure nftables is not enabled with firewalld	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.4	Ensure firewalld default zone is set	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.5	Ensure network interfaces are assigned to appropriate zone	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.6	Ensure firewalld drops unnecessary services and ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.7	Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.8	Ensure "firewalld" is installed	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.1	Ensure iptables are flushed with nftables	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.2	Ensure an nftables table exists	<input type="checkbox"/>	<input type="checkbox"/>

3.4.3.3	Ensure nftables base chains exist	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.4	Ensure nftables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.5	Ensure nftables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.6	Ensure nftables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.7	Ensure nftables service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.8	Ensure nftables rules are permanent	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.9	Ensure "nftables" is configured to allow rate limits on any connection to the system	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.1	Ensure iptables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.2	Ensure iptables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.3	Ensure iptables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.4	Ensure iptables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.5	Ensure iptables is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.1	Ensure ip6tables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.2	Ensure ip6tables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.3	Ensure ip6tables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.4	Ensure ip6tables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.5	Ensure ip6tables is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Ensure wireless interfaces are disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Disable IPv6	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure at least two name servers are configured if using DNS resolution	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure Bluetooth is disabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Ensure auditd is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Ensure auditd service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	Ensure audit_backlog_limit is sufficient	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.5	Ensure the audit service is configured to produce audit records	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.1	Ensure audit log storage size is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.2	Ensure audit logs are not automatically deleted	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.3	Ensure system is disabled when audit logs are full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.4	Ensure the operating system allocates audit record storage capacity	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.5	Ensure the operating system has the packages required for offloading audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.6	Ensure the operating system has the packages required for encrypting offloaded audit logs	<input type="checkbox"/>	<input type="checkbox"/>

4.1.2.7	Ensure the audit system off-loads audit records onto a different system or media from the system being audited	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.8	Ensure the audit system is configured to take an appropriate action when the internal event queue is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.9	Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.10	Ensure the the operating system authenticates the remote logging server for off-loading audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.11	Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure changes to system administration scope (sudoers) is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure the SA and ISSO are notified in the event of an audit processing failure	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure the SA and ISSO are notified when the audit storage volume is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure an audit event is generated for any successful/unsuccessful use of the "chage" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure the operating system is configured to audit the execution of the "fremovexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.8	Ensure the operating system is configured to audit the execution of the "fsetxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.9	Ensure the operating system is configured to audit the execution of the "lsetxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.10	Ensure the operating system is configured to audit the execution of the "removexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.11	Ensure the operating system is configured to audit the execution of the "lremovexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.12	Ensure the operating system generates audit records when successful/unsuccessful attempts to use the "su" command by performing the following command to check the file system rules in "/etc/audit/audit.rules"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.13	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.14	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.15	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.16	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd"	<input type="checkbox"/>	<input type="checkbox"/>

4.1.17	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.18	Ensure the audit system prevents unauthorized changes to logon UIDs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.19	Ensure the audit system prevents unauthorized changes	<input type="checkbox"/>	<input type="checkbox"/>
4.1.20	Ensure the operating system takes the appropriate action when the audit storage volume is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.21	Ensure the operating system takes the appropriate action when the audit storage volume is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.22	Ensure login and logout events are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.23	Ensure the operating system takes the appropriate action when an audit processing failure occurs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.24	Ensure session initiation information is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.25	Ensure events that modify date and time information are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.26	Ensure events that modify the system's Mandatory Access Controls are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.27	Ensure events that modify the system's network environment are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.28	Ensure discretionary access control permission modification events are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.29	Ensure unsuccessful unauthorized file access attempts are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.30	Ensure events that modify user/group information are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.31	Ensure successful file system mounts are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.32	Ensure use of privileged commands is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.33	Ensure file deletion events by users are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.34	Ensure kernel module loading and unloading is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.35	Ensure system administrator actions (sudolog) are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.36	Ensure the audit configuration is immutable	<input type="checkbox"/>	<input type="checkbox"/>
4.1.37	Ensure the operating system audits the execution of privileged functions	<input type="checkbox"/>	<input type="checkbox"/>
4.1.38	Ensure the operating system's audit daemon is configured to include local events	<input type="checkbox"/>	<input type="checkbox"/>
4.1.39	Ensure the operating system's audit daemon is configured to label all off-loaded audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.40	Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.41	Ensure the operating system's audit logs have a mode of "0600" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
4.1.42	Ensure the operating system's audit logs are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.43	Ensure the audit logs are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>

4.1.44	Ensure the audit log directory is owned by "root" to prevent unauthorized read access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.45	Ensure the audit log directory is group-owned by "root" to prevent unauthorized read access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.46	Ensure the audit log directories have a mode of "0700" or less permissive by first determining where the audit logs are stored	<input type="checkbox"/>	<input type="checkbox"/>
4.1.47	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chcon" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.48	Ensure the operating system is configured to audit the execution of the "setxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.49	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.50	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.51	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-agent"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.52	Ensure an audit event is generated for any successful/unsuccessful use of the "passwd" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.53	Ensure an audit event is generated for any successful/unsuccessful use of the "mount" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.54	Ensure an audit event is generated for any successful/unsuccessful use of the "umount" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.55	Ensure an audit event is generated for any successful/unsuccessful use of the "mount" syscall	<input type="checkbox"/>	<input type="checkbox"/>
4.1.56	Ensure an audit event is generated for any successful/unsuccessful use of the "unix_update"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.57	Ensure an audit event is generated for any successful/unsuccessful use of "postdrop"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.58	Ensure an audit event is generated for any successful/unsuccessful use of "postqueue"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.59	Ensure an audit event is generated for any successful/unsuccessful use of "semanage"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.60	Ensure an audit event is generated for any successful/unsuccessful use of "setfiles"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.61	Ensure an audit event is generated for any successful/unsuccessful use of "userhelper"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.62	Ensure an audit event is generated for any successful/unsuccessful use of "setsebool"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.63	Ensure an audit event is generated for any successful/unsuccessful use of "unix_chkpwd"	<input type="checkbox"/>	<input type="checkbox"/>

4.1.64	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-keysign"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.65	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "setfacl" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.66	Ensure an audit event is generated for any successful/unsuccessful use of the "pam_timestamp_check" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.67	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "newgrp" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.68	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "init_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.69	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rename" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.70	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "renameat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.71	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rmdir" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.72	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlink" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.73	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlinkat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.74	Ensure an audit event is generated for any successful/unsuccessful use of the "gpasswd" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.75	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "finit_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.76	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "delete_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.77	Ensure an audit event is generated for any successful/unsuccessful use of the "crontab" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.78	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chsh" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.79	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "truncate" command	<input type="checkbox"/>	<input type="checkbox"/>

4.1.80	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "openat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.81	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.82	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open_by_handle_at" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.83	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ftruncate" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.84	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "creat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.85	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chown" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.86	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chmod" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.87	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "lchown" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.88	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchownat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.89	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchown" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.90	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmod" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.91	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmodat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.92	Ensure an audit event is generated for any successful/unsuccessful use of the "sudo" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.93	Ensure an audit event is generated for any successful/unsuccessful use of the "usermod" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.94	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chacl" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.95	Ensure the operating system is configured to audit the execution of the module management program "kmod"	<input type="checkbox"/>	<input type="checkbox"/>

4.1.96	Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "faillock" file occur	<input type="checkbox"/>	<input type="checkbox"/>
4.1.97	Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "lastlog" file	<input type="checkbox"/>	<input type="checkbox"/>
4.1.98	Ensure the operating system enables auditing of processes that start prior to the audit daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.99	Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.100	Ensure the operating system enables Linux audit logging of the USBGuard daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.101	Ensure the files in directory "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
4.1.102	Ensure the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode	<input type="checkbox"/>	<input type="checkbox"/>
4.1.103	Ensure the audit tools are owned by "root" to prevent any unauthorized access, deletion, or modification	<input type="checkbox"/>	<input type="checkbox"/>
4.1.104	Ensure the audit tools are group-owned by "root" to prevent any unauthorized access, deletion, or modification	<input type="checkbox"/>	<input type="checkbox"/>
4.1.105	Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.1	Ensure rsyslog is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.3	Ensure the operating system monitors all remote access methods	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.4	Ensure rsyslog Service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.5	Ensure rsyslog default file permissions configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.6	Ensure logging is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.7	Ensure rsyslog is configured to send logs to a remote log host	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.8	Ensure remote rsyslog messages are only accepted on designated log hosts.	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.9	Ensure "rsyslog" is configured to log cron events	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.1	Ensure journald is configured to send logs to rsyslog	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.2	Ensure journald is configured to compress large log files	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure permissions on all logfiles are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure logrotate is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure administrators are notified if an audit processing failure occurs by modifying "/etc/aliases"	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure cron daemon is enabled	<input type="checkbox"/>	<input type="checkbox"/>

5.1.2	Ensure permissions on /etc/crontab are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on /etc/cron.hourly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure permissions on /etc/cron.daily are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure permissions on /etc/cron.weekly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure permissions on /etc/cron.monthly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure permissions on /etc/cron.d are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.8	Ensure at/cron is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure SSH private key files have a passcode	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure SSH access is limited	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure permissions on SSH private host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure permissions on SSH public host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure SSH LogLevel is appropriate	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure SSH X11 forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	Ensure SSH MaxAuthTries is set to 4 or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	Ensure SSH IgnoreRhosts is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	Ensure SSH HostbasedAuthentication is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	Ensure SSH root login is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	Ensure SSH PermitEmptyPasswords is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.2.14	Ensure SSH PermitUserEnvironment is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.15	Ensure SSH Idle Timeout Interval is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.16	Ensure SSH LoginGraceTime is set to one minute or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.17	Ensure SSH warning banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.18	Ensure SSH PAM is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.19	Ensure SSH AllowTcpForwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.20	Ensure SSH MaxStartups is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.21	Ensure SSH MaxSessions is set to 4 or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.22	Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>
5.2.23	Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>
5.2.24	Ensure the SSH server uses strong entropy	<input type="checkbox"/>	<input type="checkbox"/>
5.2.25	Ensure system-wide crypto policy is not over-ridden	<input type="checkbox"/>	<input type="checkbox"/>
5.2.26	Ensure the SSH daemon performs strict mode checking of home directory configuration files	<input type="checkbox"/>	<input type="checkbox"/>
5.2.27	Ensure the SSH daemon performs compression after a user successfully authenticates	<input type="checkbox"/>	<input type="checkbox"/>
5.2.28	Ensure the SSH daemon does not allow authentication using known host's authentication	<input type="checkbox"/>	<input type="checkbox"/>

5.2.29	Ensure the SSH daemon does not allow Kerberos authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.30	Ensure null passwords cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.2.31	Ensure SSH provides users with feedback on when account accesses last occurred	<input type="checkbox"/>	<input type="checkbox"/>
5.2.32	Ensure SSH is loaded and active	<input type="checkbox"/>	<input type="checkbox"/>
5.2.33	Ensure the SSH server is configured to force frequent session key renegotiation	<input type="checkbox"/>	<input type="checkbox"/>
5.2.34	Ensure the SSH daemon prevents remote hosts from connecting to the proxy display	<input type="checkbox"/>	<input type="checkbox"/>
5.2.35	Ensure system-wide crypto policies are in effect	<input type="checkbox"/>	<input type="checkbox"/>
5.2.36	Ensure the SSH daemon does not allow GSSAPI authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.37	Ensure SSH is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.2.38	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	Create custom authselect profile	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2	Select authselect profile	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	Ensure authselect includes with-faillock	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1	Ensure password creation requirements are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2	Ensure the system locks an account after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3	Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts within 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.4	Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.5	Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.6	Ensure lockout for failed password attempts is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.7	Ensure password reuse is limited	<input type="checkbox"/>	<input type="checkbox"/>
5.4.8	Ensure password hashing algorithm is SHA-512	<input type="checkbox"/>	<input type="checkbox"/>
5.4.9	Ensure a minimum number of hash rounds is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.10	Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes until released by an administrator	<input type="checkbox"/>	<input type="checkbox"/>
5.4.11	Ensure the "/etc/security/faillock.conf" file is configured to lock an account until released by an administrator after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.12	Ensure the faillock directory contents persist after a reboot	<input type="checkbox"/>	<input type="checkbox"/>
5.4.13	Ensure the "/etc/security/faillock.conf" file is configured to use a non-default faillock directory to ensure contents persist after reboot	<input type="checkbox"/>	<input type="checkbox"/>

5.4.14	Ensure the system prevents informative messages to the user about logon information	<input type="checkbox"/>	<input type="checkbox"/>
5.4.15	Ensure the "/etc/security/faillock.conf" file is configured to prevent informative messages about logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.16	Ensure the system logs user name information when unsuccessful logon attempts occur	<input type="checkbox"/>	<input type="checkbox"/>
5.4.17	Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur	<input type="checkbox"/>	<input type="checkbox"/>
5.4.18	Ensure the system includes the root account when locking an account after three unsuccessful logon attempts within a period of 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.19	Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur	<input type="checkbox"/>	<input type="checkbox"/>
5.4.20	Ensure the operating system prohibits password reuse for a minimum of five generations	<input type="checkbox"/>	<input type="checkbox"/>
5.4.21	Ensure the operating system uses multifactor authentication for local access to accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.22	Ensure the date and time of the last successful account logon upon logon is displayed	<input type="checkbox"/>	<input type="checkbox"/>
5.4.23	Ensure the "pam_unix.so" module is configured to use sha512	<input type="checkbox"/>	<input type="checkbox"/>
5.4.24	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/system-auth" file	<input type="checkbox"/>	<input type="checkbox"/>
5.4.25	Ensure blank or null passwords in the "system-auth" file cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.4.26	Ensure blank or null passwords in the "password-auth" file cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.4.27	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/password-auth" file	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.1	Ensure password expiration is 365 days or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.2	Ensure the shadow password suite configuration is set to encrypt password with a FIPS 140-2 approved cryptographic hashing algorithm.	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.3	Ensure the value of the "maxrepeat" option in "/etc/security/pwquality.conf" is "3"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.4	Ensure the value of the "difok" option in "/etc/security/pwquality.conf" is "8"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.5	Ensure the value of the "minclass" option in "/etc/security/pwquality.conf" is "4"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.6	Ensure the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" is "4"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.7	Ensure the value for "dcredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>

5.5.1.8	Ensure the value for "lcredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.9	Ensure the value for "ucredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.10	Ensure the operating system uses "pwquality" to enforce the password complexity rules	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.11	Ensure minimum days between password changes is 7 or more	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.12	Ensure password expiration warning days is 7 or more	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.13	Ensure inactive password lock is 30 days or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.14	Ensure all users last password change date is in the past	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.15	Ensure the minimum time period between password changes for each user account is one day or greater	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.16	Ensure the operating system enforces 24 hours/1 day as the minimum password lifetime for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.17	Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.18	Ensure the maximum time period for existing passwords is restricted to 60 days	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.19	Ensure the operating system enforces a minimum 15-character password length	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.20	Ensure the operating system enforces a minimum 15-character password length for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.21	Ensure the value for "ocredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.22	Ensure the operating system prevents the use of dictionary words for passwords	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.23	Ensure the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt	<input type="checkbox"/>	<input type="checkbox"/>
5.5.2	Ensure system accounts are secured	<input type="checkbox"/>	<input type="checkbox"/>
5.5.3	Ensure default user shell timeout is 900 seconds or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.4	Ensure the interactive user account passwords are using a strong password hash	<input type="checkbox"/>	<input type="checkbox"/>
5.5.5	Ensure default group for the root account is GID 0	<input type="checkbox"/>	<input type="checkbox"/>
5.5.6	Ensure default user umask is 027 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
5.5.7	Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.5.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
5.5.9	Ensure the default umask for all local interactive users is "077"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.10	Ensure the umask default for installed shells is "077"	<input type="checkbox"/>	<input type="checkbox"/>

5.5.11	Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files	<input type="checkbox"/>	<input type="checkbox"/>
5.6	Ensure root login is restricted to system console	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure PKI-based authentication has valid certificates	<input type="checkbox"/>	<input type="checkbox"/>
5.8	Ensure access to the su command is restricted	<input type="checkbox"/>	<input type="checkbox"/>
5.9	Ensure the operating system prevents system daemons from using Kerberos for authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.10	Ensure the krb5-workstation package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
5.11	Ensure SSSD prohibits the use of cached authentications after one day	<input type="checkbox"/>	<input type="checkbox"/>
5.12	Ensure "fapolicyd" is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.13	Ensure USBGuard has a policy configured	<input type="checkbox"/>	<input type="checkbox"/>
5.14	Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>
5.15	Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption	<input type="checkbox"/>	<input type="checkbox"/>
5.16	Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions	<input type="checkbox"/>	<input type="checkbox"/>
5.17	Ensure "fapolicyd" is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
5.18	Ensure "fapolicyd" employs a deny-all, permit-by-exception policy	<input type="checkbox"/>	<input type="checkbox"/>
5.19	Ensure USBGuard is installed on the operating system	<input type="checkbox"/>	<input type="checkbox"/>
5.20	Ensure the operating system has enabled the use of the USBGuard	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Audit system file permissions	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure permissions on /etc/passwd are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Ensure permissions on /etc/passwd- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.4	Ensure permissions on /etc/shadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.5	Ensure permissions on /etc/shadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.6	Ensure permissions on /etc/gshadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.7	Ensure permissions on /etc/gshadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.8	Ensure permissions on /etc/group are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.9	Ensure permissions on /etc/group- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.10	Ensure the root account is the only account that has unrestricted access to the operating system	<input type="checkbox"/>	<input type="checkbox"/>
6.1.11	Ensure no world writable files exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.12	Ensure no unowned files or directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.13	Ensure no ungrouped files or directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.14	Ensure all public directories are owned by root or a system account	<input type="checkbox"/>	<input type="checkbox"/>
6.1.15	Audit SUID executables	<input type="checkbox"/>	<input type="checkbox"/>
6.1.16	Audit SGID executables	<input type="checkbox"/>	<input type="checkbox"/>

6.1.17	Ensure the "/var/log/messages" file has mode "0640" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.18	Ensure the "/var/log/messages" file is owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.19	Ensure the "/var/log/messages" file is group-owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.20	Ensure the "/var/log" directory has a mode of "0755" or less	<input type="checkbox"/>	<input type="checkbox"/>
6.1.21	Ensure the "/var/log" directory is owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.22	Ensure the "/var/log" directory is group-owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.23	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories have mode "0755" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.24	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.25	Ensure the system commands contained in "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.26	Ensure the system-wide shared library files contained in the "/lib, /lib64, /usr/lib, /usr/lib64" directories have mode "0755" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.27	Ensure the system-wide shared library files are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.28	Ensure the system-wide shared library files are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.29	Ensure world-writable directories are owned by root, sys, bin, or an application user	<input type="checkbox"/>	<input type="checkbox"/>
6.1.30	Ensure world-writable directories are group-owned by root, sys, bin, or an application group	<input type="checkbox"/>	<input type="checkbox"/>
6.1.31	Ensure local initialization files do not execute world-writable programs	<input type="checkbox"/>	<input type="checkbox"/>
6.1.32	Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer	<input type="checkbox"/>	<input type="checkbox"/>
6.1.33	Ensure the operating system prevents users from disabling the tmux terminal multiplexer	<input type="checkbox"/>	<input type="checkbox"/>
6.1.34	Ensure the operating system enables a user's session lock until that user re-establishes access	<input type="checkbox"/>	<input type="checkbox"/>
6.1.35	Ensure the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
6.1.36	Ensure the operating system initiates a session lock after 15 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
6.1.37	Ensure all accounts on the system are assigned to an active system, application, or user account	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1	Ensure password fields are not empty	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Ensure root PATH Integrity	<input type="checkbox"/>	<input type="checkbox"/>

6.2.4	Ensure no legacy "+" entries exist in /etc/shadow	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure no legacy "+" entries exist in /etc/group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure root is the only UID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure users' home directories permissions are 750 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
6.2.9	Ensure users own their home directories	<input type="checkbox"/>	<input type="checkbox"/>
6.2.10	Ensure users' dot files are not group or world writable	<input type="checkbox"/>	<input type="checkbox"/>
6.2.11	Ensure no users have .forward files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.12	Ensure no users have .netrc files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.13	Ensure users' .netrc Files are not group or world accessible	<input type="checkbox"/>	<input type="checkbox"/>
6.2.14	Ensure no users have .rhosts files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.15	Ensure all groups in /etc/passwd exist in /etc/group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.16	Ensure no duplicate UIDs exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.17	Ensure no duplicate GIDs exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.18	Ensure no duplicate user names exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.19	Ensure no duplicate group names exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.20	Ensure shadow group is empty	<input type="checkbox"/>	<input type="checkbox"/>
6.2.21	Ensure all users' home directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.22	Ensure the assigned home directory of all local interactive users is group-owned by that user's primary GID	<input type="checkbox"/>	<input type="checkbox"/>
6.2.23	Ensure the assigned home directory of all local interactive users exists	<input type="checkbox"/>	<input type="checkbox"/>
6.2.24	Ensure all local interactive users are assigned a home directory upon creation	<input type="checkbox"/>	<input type="checkbox"/>
6.2.25	Ensure all local initialization files have a mode of "0740" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.2.26	Ensure all local files and directories have a valid owner	<input type="checkbox"/>	<input type="checkbox"/>
6.2.27	Ensure all local files and directories have a valid group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.28	Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file	<input type="checkbox"/>	<input type="checkbox"/>
6.2.29	Ensure file executable search path statements do not share sensitive home directory information	<input type="checkbox"/>	<input type="checkbox"/>
6.2.30	Ensure local interactive users have a home directory assigned	<input type="checkbox"/>	<input type="checkbox"/>
6.2.31	Ensure the operating system limits the number of concurrent sessions to "10" for all accounts and/or account types	<input type="checkbox"/>	<input type="checkbox"/>
6.2.32	Ensure the operating system enables a user's session lock until that user re-establishes access	<input type="checkbox"/>	<input type="checkbox"/>
6.2.33	Ensure the operating system enables the user to initiate a session lock	<input type="checkbox"/>	<input type="checkbox"/>
6.2.34	Ensure the operating system prevents a user from overriding settings for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>

6.2.35	Ensure all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750"	<input type="checkbox"/>	<input type="checkbox"/>
6.2.36	Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of	<input type="checkbox"/>	<input type="checkbox"/>
6.2.37	Ensure temporary accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure the operating system removes all software components after updated versions have been installed	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure there are no ".shosts" files on the operating system	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Ensure there are no "shosts.equiv" files on the operating system	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of cramfs filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure mounting of vFAT filesystems is limited	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure mounting of squashfs filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure mounting of udf filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Ensure /tmp is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Ensure nodev option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Ensure nosuid option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Ensure noexec option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	Ensure separate partition exists for /var	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Ensure separate partition exists for /var/tmp	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Ensure nodev option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Ensure nosuid option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Ensure noexec option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.11	Ensure separate partition exists for /var/log	<input type="checkbox"/>	<input type="checkbox"/>
1.1.12	Ensure separate partition exists for /var/log/audit	<input type="checkbox"/>	<input type="checkbox"/>
1.1.13	Ensure separate partition exists for /home	<input type="checkbox"/>	<input type="checkbox"/>
1.1.14	Ensure nodev option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.15	Ensure nodev option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.16	Ensure nosuid option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.17	Ensure noexec option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.18	Ensure nodev option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.19	Ensure nosuid option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.20	Ensure noexec option set on removable media partitions	<input type="checkbox"/>	<input type="checkbox"/>
1.1.21	Ensure sticky bit is set on all world-writable directories	<input type="checkbox"/>	<input type="checkbox"/>
1.1.22	Disable Automounting	<input type="checkbox"/>	<input type="checkbox"/>
1.1.23	Disable USB Storage	<input type="checkbox"/>	<input type="checkbox"/>
1.1.24	Ensure file systems that contain user home directories are mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.25	Ensure the "/boot" directory is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.26	Ensure all non-root local partitions are mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.27	Ensure file systems that are being NFS-imported are mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.29	Ensure file systems being imported via NFS are mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>

1.1.30	Ensure a separate file system/partition has been created for non-privileged local interactive user home directories	<input type="checkbox"/>	<input type="checkbox"/>
1.1.31	Ensure "/var/log" is mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.32	Ensure "/var/log" is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.33	Ensure "/var/log" is mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.34	Ensure "/var/log/audit" is mounted with the "nodev" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.35	Ensure "/var/log/audit" is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.36	Ensure "/var/log/audit" is mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.37	Ensure the "/boot/efi" directory is mounted with the "nosuid" option	<input type="checkbox"/>	<input type="checkbox"/>
1.1.38	Ensure file systems that contain user home directories are mounted with the "noexec" option	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1	Ensure GPG keys are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Ensure gpgcheck is globally activated	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Ensure package manager repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Ensure DNF is configured to perform a signature check on local packages	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Ensure sudo is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
1.3.3	Ensure sudo log file exists	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Ensure the "/etc/sudoers" file has no occurrences of "NOPASSWD"	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	Ensure the "/etc/sudoers" file has no occurrences of "!authenticate"	<input type="checkbox"/>	<input type="checkbox"/>
1.3.6	Ensure the "sudoers" file restricts sudo access to authorized personnel	<input type="checkbox"/>	<input type="checkbox"/>
1.3.7	Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation	<input type="checkbox"/>	<input type="checkbox"/>
1.3.8	Ensure the operating system requires re-authentication when using the "sudo" command to elevate privileges	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure AIDE is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure filesystem integrity is regularly checked	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Ensure Advanced Intrusion Detection Environment (AIDE) is properly configured to use cryptographic mechanisms to protect the integrity of audit tools	<input type="checkbox"/>	<input type="checkbox"/>
1.4.4	Ensure the file integrity tool is configured to verify extended attributes	<input type="checkbox"/>	<input type="checkbox"/>
1.4.5	Ensure the file integrity tool is configured to verify ACLs	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure permissions on bootloader config are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure bootloader password is set	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Ensure authentication required for single user mode	<input type="checkbox"/>	<input type="checkbox"/>

1.5.4	Ensure the encrypted grub superusers password is set for systems booted with UEFI	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Ensure the encrypted grub superusers password is set for system booted with BIOS	<input type="checkbox"/>	<input type="checkbox"/>
1.5.6	Ensure the operating system requires authentication for rescue mode	<input type="checkbox"/>	<input type="checkbox"/>
1.5.7	Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities	<input type="checkbox"/>	<input type="checkbox"/>
1.5.8	Ensure GRUB 2 is configured to disable vsyscalls	<input type="checkbox"/>	<input type="checkbox"/>
1.5.9	Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities	<input type="checkbox"/>	<input type="checkbox"/>
1.5.10	Ensure the operating system is configured to boot to the command line	<input type="checkbox"/>	<input type="checkbox"/>
1.5.11	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed	<input type="checkbox"/>	<input type="checkbox"/>
1.5.12	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds	<input type="checkbox"/>	<input type="checkbox"/>
1.5.13	Ensure a unique name is set as the "superusers" account (UEFI)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.14	Ensure a unique name is set as the "superusers" account (BIOS)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.15	Ensure the operating system requires authentication upon booting into emergency mode	<input type="checkbox"/>	<input type="checkbox"/>
1.6.1	Ensure core dumps are restricted	<input type="checkbox"/>	<input type="checkbox"/>
1.6.2	Ensure address space layout randomization (ASLR) is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure the operating system is not configured to acquire, save, or process core dumps	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure kernel core dumps are disabled unless needed	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure the operating system disables core dumps for all users	<input type="checkbox"/>	<input type="checkbox"/>
1.6.7	Ensure the operating system disables storing core dumps for all users	<input type="checkbox"/>	<input type="checkbox"/>
1.6.8	Ensure the operating system disables core dump backtraces	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.1	Ensure SELinux is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.2	Ensure SELinux is not disabled in bootloader configuration	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.3	Ensure SELinux policy is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.4	Ensure the SELinux state is enforcing	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.5	Ensure no unconfined services exist	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.6	Ensure SETroubleshoot is not installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.7	Ensure the MCS Translation Service (mcstrans) is not installed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1.8	Ensure the operating system has the policycoreutils package installed	<input type="checkbox"/>	<input type="checkbox"/>

1.8.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.8.2	Ensure message of the day is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.3	Ensure local login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.4	Ensure remote login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.8.5	Ensure permissions on /etc/motd are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.6	Ensure permissions on /etc/issue are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.7	Ensure permissions on /etc/issue.net are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.8.8	Ensure the Standard Mandatory DoD Notice and Consent Banner is displayed before granting access to the system via SSH logon	<input type="checkbox"/>	<input type="checkbox"/>
1.8.9	Ensure the operating system displays a banner before granting access to the operating system via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.1	Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.2	Ensure GNOME Display Manager is removed	<input type="checkbox"/>	<input type="checkbox"/>
1.9.3	Ensure GDM login banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.9.4	Ensure last logged in user display is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.9.5	Ensure XDCMP is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.9.6	Ensure a Standard Mandatory DoD Notice and Consent Banner is displayed via a graphical user logon	<input type="checkbox"/>	<input type="checkbox"/>
1.9.7	Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.8	Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.9	Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated	<input type="checkbox"/>	<input type="checkbox"/>
1.9.10	Ensure the operating system disables the user logon list for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
1.9.11	Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.9.12	Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface	<input type="checkbox"/>	<input type="checkbox"/>
1.10	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure system-wide crypto policy is not legacy	<input type="checkbox"/>	<input type="checkbox"/>
1.12	Ensure system-wide crypto policy is FUTURE or FIPS	<input type="checkbox"/>	<input type="checkbox"/>

1.13	Ensure the operating system implements DoD-approved encryption	<input type="checkbox"/>	<input type="checkbox"/>
1.14	Ensure the operating system prevents unauthorized modification of all information at rest by using disk encryption	<input type="checkbox"/>	<input type="checkbox"/>
1.15	Ensure kernel image loading is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure the operating system is configured to enable DAC on symlinks	<input type="checkbox"/>	<input type="checkbox"/>
1.17	Ensure the operating system is configured to enable DAC on hardlinks	<input type="checkbox"/>	<input type="checkbox"/>
1.18	Ensure the operating system is configured to restrict access to the kernel message buffer	<input type="checkbox"/>	<input type="checkbox"/>
1.19	Ensure the operating system is configured to prevent kernel profiling by unprivileged users	<input type="checkbox"/>	<input type="checkbox"/>
1.20	Ensure the operating system has the packages required for multifactor authentication	<input type="checkbox"/>	<input type="checkbox"/>
1.21	Ensure the operating system implements certificate status checking for multifactor authentication	<input type="checkbox"/>	<input type="checkbox"/>
1.22	Ensure the operating system accepts PIV credentials	<input type="checkbox"/>	<input type="checkbox"/>
1.23	Ensure the NX (no-execution) bit flag is set on the system	<input type="checkbox"/>	<input type="checkbox"/>
1.24	Ensure kernel page-table isolation is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.25	Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall	<input type="checkbox"/>	<input type="checkbox"/>
1.26	Ensure the operating system restricts usage of ptrace to descendant processes	<input type="checkbox"/>	<input type="checkbox"/>
1.27	Ensure the operating system restricts exposed kernel pointer addresses access	<input type="checkbox"/>	<input type="checkbox"/>
1.28	Ensure the operating system disables the ability to load the firewire-core kernel module	<input type="checkbox"/>	<input type="checkbox"/>
1.29	Ensure the operating system disables the ability to load the USB Storage kernel module	<input type="checkbox"/>	<input type="checkbox"/>
1.30	Ensure the operating system disables the use of user namespaces	<input type="checkbox"/>	<input type="checkbox"/>
1.31	Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service	<input type="checkbox"/>	<input type="checkbox"/>
1.32	Ensure the "tmux" package installed	<input type="checkbox"/>	<input type="checkbox"/>
1.33	Ensure the operating system enables hardening for the BPF JIT	<input type="checkbox"/>	<input type="checkbox"/>
1.34	Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	Ensure xinetd is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.1	Ensure time synchronization is in use	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.2	Ensure chrony is configured	<input type="checkbox"/>	<input type="checkbox"/>

2.2.1.3	Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.4	Ensure the operating system disables the chrony daemon from acting as a server	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.5	Ensure the operating system disables network management of the chrony daemon	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure X Window System is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure rsync service is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure Avahi Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure SNMP Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure HTTP Proxy Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Ensure Samba is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Ensure IMAP and POP3 server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	Ensure HTTP server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	Ensure FTP Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure DNS Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.12	Ensure NFS is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure RPC is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	Ensure LDAP server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	Ensure DHCP Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	Ensure the telnet-server package is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.17	Ensure CUPS is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.18	Ensure NIS Server is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.19	Ensure mail transfer agent is configured for local-only mode	<input type="checkbox"/>	<input type="checkbox"/>
2.2.20	Ensure the operating system has enabled the hardware random number generator entropy gatherer service	<input type="checkbox"/>	<input type="checkbox"/>
2.2.21	Ensure automated bug reporting tools are not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.22	Ensure the sendmail package is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.23	Ensure the rsh-server package is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.24	Ensure a camera is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.25	Ensure the operating system is configured to mask the debug-shell systemd service	<input type="checkbox"/>	<input type="checkbox"/>
2.2.26	Ensure a TFTP server has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.27	Ensure the operating system is configured to prevent unrestricted mail relaying	<input type="checkbox"/>	<input type="checkbox"/>
2.2.28	Ensure the TFTP daemon is configured to operate in secure mode	<input type="checkbox"/>	<input type="checkbox"/>
2.2.29	Ensure an FTP server has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.30	Ensure the gssproxy package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.31	Ensure the iputils package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.2.32	Ensure the tuned package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>

2.2.33	Ensure the krb5-server package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure NIS Client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure telnet client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure LDAP client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure IP forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure the system does not accept router advertisements on IPv6 interfaces, unless the system is a router	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Ensure the system does not accept router advertisements on IPv6 interfaces by default, unless the system is a router	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure Reverse Path Filtering is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.8	Ensure TCP SYN Cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.9	Ensure IPv6 router advertisements are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.10	Ensure the operating system does not accept IPv6 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.11	Ensure the operating system does not accept IPv6 source-routed packets	<input type="checkbox"/>	<input type="checkbox"/>
3.2.12	Ensure the operating system does not accept IPv6 source-routed packets by default	<input type="checkbox"/>	<input type="checkbox"/>
3.2.13	Ensure the operating system ignores IPv6 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.14	Ensure network interfaces are not in promiscuous mode	<input type="checkbox"/>	<input type="checkbox"/>
3.2.15	Ensure the operating system does not accept IPv4 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.2.16	Ensure the operating system does not accept IPv4 source-routed packet	<input type="checkbox"/>	<input type="checkbox"/>
3.2.17	Ensure the operating system does not accept IPv4 source-routed packets by default	<input type="checkbox"/>	<input type="checkbox"/>
3.2.18	Ensure the operating system ignores IPv4 ICMP redirect messages	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure DCCP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure SCTP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure RDS is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure TIPC is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure ATM is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure CAN is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.1	Ensure a Firewall package is installed	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.1	Ensure firewalld service is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>

3.4.2.2	Ensure iptables service is not enabled with firewalld	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.3	Ensure nftables is not enabled with firewalld	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.4	Ensure firewalld default zone is set	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.5	Ensure network interfaces are assigned to appropriate zone	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.6	Ensure firewalld drops unnecessary services and ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.7	Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.8	Ensure "firewalld" is installed	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.1	Ensure iptables are flushed with nftables	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.2	Ensure an nftables table exists	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.3	Ensure nftables base chains exist	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.4	Ensure nftables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.5	Ensure nftables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.6	Ensure nftables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.7	Ensure nftables service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.8	Ensure nftables rules are permanent	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3.9	Ensure "nftables" is configured to allow rate limits on any connection to the system	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.1	Ensure iptables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.2	Ensure iptables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.3	Ensure iptables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.4	Ensure iptables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.1.5	Ensure iptables is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.1	Ensure ip6tables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.2	Ensure ip6tables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.3	Ensure ip6tables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.4	Ensure ip6tables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4.2.5	Ensure ip6tables is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Ensure wireless interfaces are disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Disable IPv6	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure at least two name servers are configured if using DNS resolution	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure Bluetooth is disabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Ensure auditd is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Ensure auditd service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	Ensure audit_backlog_limit is sufficient	<input type="checkbox"/>	<input type="checkbox"/>

4.1.1.5	Ensure the audit service is configured to produce audit records	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.1	Ensure audit log storage size is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.2	Ensure audit logs are not automatically deleted	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.3	Ensure system is disabled when audit logs are full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.4	Ensure the operating system allocates audit record storage capacity	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.5	Ensure the operating system has the packages required for offloading audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.6	Ensure the operating system has the packages required for encrypting offloaded audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.7	Ensure the audit system off-loads audit records onto a different system or media from the system being audited	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.8	Ensure the audit system is configured to take an appropriate action when the internal event queue is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.9	Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.10	Ensure the the operating system authenticates the remote logging server for off-loading audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.11	Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure changes to system administration scope (sudoers) is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure the SA and ISSO are notified in the event of an audit processing failure	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure the SA and ISSO are notified when the audit storage volume is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure an audit event is generated for any successful/unsuccessful use of the "chage" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure the operating system is configured to audit the execution of the "fremovexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.8	Ensure the operating system is configured to audit the execution of the "fsetxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.9	Ensure the operating system is configured to audit the execution of the "lsetxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.10	Ensure the operating system is configured to audit the execution of the "removexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.11	Ensure the operating system is configured to audit the execution of the "lremovexattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.12	Ensure the operating system generates audit records when successful/unsuccessful attempts to use the "su" command by performing the following command to check the file system rules in "/etc/audit/audit.rules"	<input type="checkbox"/>	<input type="checkbox"/>

4.1.13	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.14	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.15	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.16	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.17	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.18	Ensure the audit system prevents unauthorized changes to logon UIDs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.19	Ensure the audit system prevents unauthorized changes	<input type="checkbox"/>	<input type="checkbox"/>
4.1.20	Ensure the operating system takes the appropriate action when the audit storage volume is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.21	Ensure the operating system takes the appropriate action when the audit storage volume is full	<input type="checkbox"/>	<input type="checkbox"/>
4.1.22	Ensure login and logout events are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.23	Ensure the operating system takes the appropriate action when an audit processing failure occurs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.24	Ensure session initiation information is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.25	Ensure events that modify date and time information are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.26	Ensure events that modify the system's Mandatory Access Controls are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.27	Ensure events that modify the system's network environment are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.28	Ensure discretionary access control permission modification events are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.29	Ensure unsuccessful unauthorized file access attempts are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.30	Ensure events that modify user/group information are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.31	Ensure successful file system mounts are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.32	Ensure use of privileged commands is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.33	Ensure file deletion events by users are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.34	Ensure kernel module loading and unloading is collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.35	Ensure system administrator actions (sudolog) are collected	<input type="checkbox"/>	<input type="checkbox"/>
4.1.36	Ensure the audit configuration is immutable	<input type="checkbox"/>	<input type="checkbox"/>

4.1.37	Ensure the operating system audits the execution of privileged functions	<input type="checkbox"/>	<input type="checkbox"/>
4.1.38	Ensure the operating system's audit daemon is configured to include local events	<input type="checkbox"/>	<input type="checkbox"/>
4.1.39	Ensure the operating system's audit daemon is configured to label all off-loaded audit logs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.40	Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.41	Ensure the operating system's audit logs have a mode of "0600" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
4.1.42	Ensure the operating system's audit logs are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.43	Ensure the audit logs are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.44	Ensure the audit log directory is owned by "root" to prevent unauthorized read access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.45	Ensure the audit log directory is group-owned by "root" to prevent unauthorized read access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.46	Ensure the audit log directories have a mode of "0700" or less permissive by first determining where the audit logs are stored	<input type="checkbox"/>	<input type="checkbox"/>
4.1.47	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chcon" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.48	Ensure the operating system is configured to audit the execution of the "setxattr" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.49	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.50	Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.51	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-agent"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.52	Ensure an audit event is generated for any successful/unsuccessful use of the "passwd" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.53	Ensure an audit event is generated for any successful/unsuccessful use of the "mount" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.54	Ensure an audit event is generated for any successful/unsuccessful use of the "umount" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.55	Ensure an audit event is generated for any successful/unsuccessful use of the "mount" syscall	<input type="checkbox"/>	<input type="checkbox"/>
4.1.56	Ensure an audit event is generated for any successful/unsuccessful use of the "unix_update"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.57	Ensure an audit event is generated for any successful/unsuccessful use of "postdrop"	<input type="checkbox"/>	<input type="checkbox"/>

4.1.58	Ensure an audit event is generated for any successful/unsuccessful use of "postqueue"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.59	Ensure an audit event is generated for any successful/unsuccessful use of "semanage"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.60	Ensure an audit event is generated for any successful/unsuccessful use of "setfiles"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.61	Ensure an audit event is generated for any successful/unsuccessful use of "userhelper"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.62	Ensure an audit event is generated for any successful/unsuccessful use of "setsebool"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.63	Ensure an audit event is generated for any successful/unsuccessful use of "unix_chkpwd"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.64	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ssh-keysign" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.65	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "setfacl" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.66	Ensure an audit event is generated for any successful/unsuccessful use of the "pam_timestamp_check" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.67	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "newgrp" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.68	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "init_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.69	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rename" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.70	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "renameat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.71	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "rmdir" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.72	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlink" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.73	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "unlinkat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.74	Ensure an audit event is generated for any successful/unsuccessful use of the "gpasswd" command	<input type="checkbox"/>	<input type="checkbox"/>

4.1.75	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "finit_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.76	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "delete_module" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.77	Ensure an audit event is generated for any successful/unsuccessful use of the "crontab" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.78	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chsh" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.79	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "truncate" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.80	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "openat" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.81	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.82	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "open_by_handle_at" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.83	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "ftruncate" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.84	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "creat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.85	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chown" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.86	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chmod" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.87	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "lchown" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.88	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchownat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.89	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchown" system call	<input type="checkbox"/>	<input type="checkbox"/>

4.1.90	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmod" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.91	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "fchmodat" system call	<input type="checkbox"/>	<input type="checkbox"/>
4.1.92	Ensure an audit event is generated for any successful/unsuccessful use of the "sudo" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.93	Ensure an audit event is generated for any successful/unsuccessful use of the "usermod" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.94	Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the "chacl" command	<input type="checkbox"/>	<input type="checkbox"/>
4.1.95	Ensure the operating system is configured to audit the execution of the module management program "kmod"	<input type="checkbox"/>	<input type="checkbox"/>
4.1.96	Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "faillock" file occur	<input type="checkbox"/>	<input type="checkbox"/>
4.1.97	Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the "lastlog" file	<input type="checkbox"/>	<input type="checkbox"/>
4.1.98	Ensure the operating system enables auditing of processes that start prior to the audit daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.99	Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.100	Ensure the operating system enables Linux audit logging of the USBGuard daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.101	Ensure the files in directory "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
4.1.102	Ensure the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode	<input type="checkbox"/>	<input type="checkbox"/>
4.1.103	Ensure the audit tools are owned by "root" to prevent any unauthorized access, deletion, or modification	<input type="checkbox"/>	<input type="checkbox"/>
4.1.104	Ensure the audit tools are group-owned by "root" to prevent any unauthorized access, deletion, or modification	<input type="checkbox"/>	<input type="checkbox"/>
4.1.105	Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.1	Ensure rsyslog is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.3	Ensure the operating system monitors all remote access methods	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.4	Ensure rsyslog Service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.5	Ensure rsyslog default file permissions configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.6	Ensure logging is configured	<input type="checkbox"/>	<input type="checkbox"/>

4.2.1.7	Ensure rsyslog is configured to send logs to a remote log host	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.8	Ensure remote rsyslog messages are only accepted on designated log hosts.	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.9	Ensure "rsyslog" is configured to log cron events	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.1	Ensure journald is configured to send logs to rsyslog	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.2	Ensure journald is configured to compress large log files	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure permissions on all logfiles are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure logrotate is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure administrators are notified if an audit processing failure occurs by modifying "/etc/aliases"	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure cron daemon is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure permissions on /etc/crontab are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on /etc/cron.hourly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure permissions on /etc/cron.daily are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure permissions on /etc/cron.weekly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure permissions on /etc/cron.monthly are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure permissions on /etc/cron.d are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.8	Ensure at/cron is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure SSH private key files have a passcode	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure SSH access is limited	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure permissions on SSH private host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure permissions on SSH public host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure SSH LogLevel is appropriate	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure SSH X11 forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	Ensure SSH MaxAuthTries is set to 4 or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	Ensure SSH IgnoreRhosts is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	Ensure SSH HostbasedAuthentication is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	Ensure SSH root login is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	Ensure SSH PermitEmptyPasswords is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.2.14	Ensure SSH PermitUserEnvironment is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.15	Ensure SSH Idle Timeout Interval is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.16	Ensure SSH LoginGraceTime is set to one minute or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.17	Ensure SSH warning banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.18	Ensure SSH PAM is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.19	Ensure SSH AllowTcpForwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>

5.2.20	Ensure SSH MaxStartups is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.2.21	Ensure SSH MaxSessions is set to 4 or less	<input type="checkbox"/>	<input type="checkbox"/>
5.2.22	Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>
5.2.23	Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>
5.2.24	Ensure the SSH server uses strong entropy	<input type="checkbox"/>	<input type="checkbox"/>
5.2.25	Ensure system-wide crypto policy is not over-ridden	<input type="checkbox"/>	<input type="checkbox"/>
5.2.26	Ensure the SSH daemon performs strict mode checking of home directory configuration files	<input type="checkbox"/>	<input type="checkbox"/>
5.2.27	Ensure the SSH daemon performs compression after a user successfully authenticates	<input type="checkbox"/>	<input type="checkbox"/>
5.2.28	Ensure the SSH daemon does not allow authentication using known host's authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.29	Ensure the SSH daemon does not allow Kerberos authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.30	Ensure null passwords cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.2.31	Ensure SSH provides users with feedback on when account accesses last occurred	<input type="checkbox"/>	<input type="checkbox"/>
5.2.32	Ensure SSH is loaded and active	<input type="checkbox"/>	<input type="checkbox"/>
5.2.33	Ensure the SSH server is configured to force frequent session key renegotiation	<input type="checkbox"/>	<input type="checkbox"/>
5.2.34	Ensure the SSH daemon prevents remote hosts from connecting to the proxy display	<input type="checkbox"/>	<input type="checkbox"/>
5.2.35	Ensure system-wide crypto policies are in effect	<input type="checkbox"/>	<input type="checkbox"/>
5.2.36	Ensure the SSH daemon does not allow GSSAPI authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.2.37	Ensure SSH is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.2.38	Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	Create custom authselect profile	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2	Select authselect profile	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	Ensure authselect includes with-faillock	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1	Ensure password creation requirements are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2	Ensure the system locks an account after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3	Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts within 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.4	Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.5	Ensure the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.6	Ensure lockout for failed password attempts is configured	<input type="checkbox"/>	<input type="checkbox"/>

5.4.7	Ensure password reuse is limited	<input type="checkbox"/>	<input type="checkbox"/>
5.4.8	Ensure password hashing algorithm is SHA-512	<input type="checkbox"/>	<input type="checkbox"/>
5.4.9	Ensure a minimum number of hash rounds is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.10	Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes until released by an administrator	<input type="checkbox"/>	<input type="checkbox"/>
5.4.11	Ensure the "/etc/security/faillock.conf" file is configured to lock an account until released by an administrator after three unsuccessful logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.12	Ensure the faillock directory contents persist after a reboot	<input type="checkbox"/>	<input type="checkbox"/>
5.4.13	Ensure the "/etc/security/faillock.conf" file is configured to use a non-default faillock directory to ensure contents persist after reboot	<input type="checkbox"/>	<input type="checkbox"/>
5.4.14	Ensure the system prevents informative messages to the user about logon information	<input type="checkbox"/>	<input type="checkbox"/>
5.4.15	Ensure the "/etc/security/faillock.conf" file is configured to prevent informative messages about logon attempts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.16	Ensure the system logs user name information when unsuccessful logon attempts occur	<input type="checkbox"/>	<input type="checkbox"/>
5.4.17	Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur	<input type="checkbox"/>	<input type="checkbox"/>
5.4.18	Ensure the system includes the root account when locking an account after three unsuccessful logon attempts within a period of 15 minutes	<input type="checkbox"/>	<input type="checkbox"/>
5.4.19	Ensure the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur	<input type="checkbox"/>	<input type="checkbox"/>
5.4.20	Ensure the operating system prohibits password reuse for a minimum of five generations	<input type="checkbox"/>	<input type="checkbox"/>
5.4.21	Ensure the operating system uses multifactor authentication for local access to accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.4.22	Ensure the date and time of the last successful account logon upon logon is displayed	<input type="checkbox"/>	<input type="checkbox"/>
5.4.23	Ensure the "pam_unix.so" module is configured to use sha512	<input type="checkbox"/>	<input type="checkbox"/>
5.4.24	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/system-auth" file	<input type="checkbox"/>	<input type="checkbox"/>
5.4.25	Ensure blank or null passwords in the "system-auth" file cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.4.26	Ensure blank or null passwords in the "password-auth" file cannot be used	<input type="checkbox"/>	<input type="checkbox"/>
5.4.27	Ensure the "pam_faillock.so" module is present in the "/etc/pam.d/password-auth" file	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.1	Ensure password expiration is 365 days or less	<input type="checkbox"/>	<input type="checkbox"/>

5.5.1.2	Ensure the shadow password suite configuration is set to encrypt password with a FIPS 140-2 approved cryptographic hashing algorithm.	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.3	Ensure the value of the "maxrepeat" option in "/etc/security/pwquality.conf" is "3"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.4	Ensure the value of the "difok" option in "/etc/security/pwquality.conf" is "8"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.5	Ensure the value of the "minclass" option in "/etc/security/pwquality.conf" is "4"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.6	Ensure the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" is "4"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.7	Ensure the value for "dcredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.8	Ensure the value for "lcredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.9	Ensure the value for "ucredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.10	Ensure the operating system uses "pwquality" to enforce the password complexity rules	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.11	Ensure minimum days between password changes is 7 or more	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.12	Ensure password expiration warning days is 7 or more	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.13	Ensure inactive password lock is 30 days or less	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.14	Ensure all users last password change date is in the past	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.15	Ensure the minimum time period between password changes for each user account is one day or greater	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.16	Ensure the operating system enforces 24 hours/1 day as the minimum password lifetime for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.17	Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.18	Ensure the maximum time period for existing passwords is restricted to 60 days	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.19	Ensure the operating system enforces a minimum 15-character password length	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.20	Ensure the operating system enforces a minimum 15-character password length for new user accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.21	Ensure the value for "ocredit" in "/etc/security/pwquality.conf" is "-1"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.22	Ensure the operating system prevents the use of dictionary words for passwords	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.23	Ensure the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt	<input type="checkbox"/>	<input type="checkbox"/>
5.5.2	Ensure system accounts are secured	<input type="checkbox"/>	<input type="checkbox"/>
5.5.3	Ensure default user shell timeout is 900 seconds or less	<input type="checkbox"/>	<input type="checkbox"/>

5.5.4	Ensure the interactive user account passwords are using a strong password hash	<input type="checkbox"/>	<input type="checkbox"/>
5.5.5	Ensure default group for the root account is GID 0	<input type="checkbox"/>	<input type="checkbox"/>
5.5.6	Ensure default user umask is 027 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
5.5.7	Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
5.5.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
5.5.9	Ensure the default umask for all local interactive users is "077"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.10	Ensure the umask default for installed shells is "077"	<input type="checkbox"/>	<input type="checkbox"/>
5.5.11	Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files	<input type="checkbox"/>	<input type="checkbox"/>
5.6	Ensure root login is restricted to system console	<input type="checkbox"/>	<input type="checkbox"/>
5.7	Ensure PKI-based authentication has valid certificates	<input type="checkbox"/>	<input type="checkbox"/>
5.8	Ensure access to the su command is restricted	<input type="checkbox"/>	<input type="checkbox"/>
5.9	Ensure the operating system prevents system daemons from using Kerberos for authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.10	Ensure the krb5-workstation package has not been installed on the system	<input type="checkbox"/>	<input type="checkbox"/>
5.11	Ensure SSSD prohibits the use of cached authentications after one day	<input type="checkbox"/>	<input type="checkbox"/>
5.12	Ensure "fapolicyd" is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.13	Ensure USBGuard has a policy configured	<input type="checkbox"/>	<input type="checkbox"/>
5.14	Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms	<input type="checkbox"/>	<input type="checkbox"/>
5.15	Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption	<input type="checkbox"/>	<input type="checkbox"/>
5.16	Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions	<input type="checkbox"/>	<input type="checkbox"/>
5.17	Ensure "fapolicyd" is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
5.18	Ensure "fapolicyd" employs a deny-all, permit-by-exception policy	<input type="checkbox"/>	<input type="checkbox"/>
5.19	Ensure USBGuard is installed on the operating system	<input type="checkbox"/>	<input type="checkbox"/>
5.20	Ensure the operating system has enabled the use of the USBGuard	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Audit system file permissions	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure permissions on /etc/passwd are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Ensure permissions on /etc/passwd- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.4	Ensure permissions on /etc/shadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.5	Ensure permissions on /etc/shadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.6	Ensure permissions on /etc/gshadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.7	Ensure permissions on /etc/gshadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.8	Ensure permissions on /etc/group are configured	<input type="checkbox"/>	<input type="checkbox"/>

6.1.9	Ensure permissions on /etc/group- are configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.10	Ensure the root account is the only account that has unrestricted access to the operating system	<input type="checkbox"/>	<input type="checkbox"/>
6.1.11	Ensure no world writable files exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.12	Ensure no unowned files or directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.13	Ensure no ungrouped files or directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.1.14	Ensure all public directories are owned by root or a system account	<input type="checkbox"/>	<input type="checkbox"/>
6.1.15	Audit SUID executables	<input type="checkbox"/>	<input type="checkbox"/>
6.1.16	Audit SGID executables	<input type="checkbox"/>	<input type="checkbox"/>
6.1.17	Ensure the "/var/log/messages" file has mode "0640" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.18	Ensure the "/var/log/messages" file is owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.19	Ensure the "/var/log/messages" file is group-owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.20	Ensure the "/var/log" directory has a mode of "0755" or less	<input type="checkbox"/>	<input type="checkbox"/>
6.1.21	Ensure the "/var/log" directory is owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.22	Ensure the "/var/log" directory is group-owned by root	<input type="checkbox"/>	<input type="checkbox"/>
6.1.23	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories have mode "0755" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.24	Ensure the system commands contained in the "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.25	Ensure the system commands contained in "/bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin" directories are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.26	Ensure the system-wide shared library files contained in the "/lib, /lib64, /usr/lib, /usr/lib64" directories have mode "0755" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.1.27	Ensure the system-wide shared library files are owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.28	Ensure the system-wide shared library files are group-owned by "root"	<input type="checkbox"/>	<input type="checkbox"/>
6.1.29	Ensure world-writable directories are owned by root, sys, bin, or an application user	<input type="checkbox"/>	<input type="checkbox"/>
6.1.30	Ensure world-writable directories are group-owned by root, sys, bin, or an application group	<input type="checkbox"/>	<input type="checkbox"/>
6.1.31	Ensure local initialization files do not execute world-writable programs	<input type="checkbox"/>	<input type="checkbox"/>
6.1.32	Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer	<input type="checkbox"/>	<input type="checkbox"/>
6.1.33	Ensure the operating system prevents users from disabling the tmux terminal multiplexer	<input type="checkbox"/>	<input type="checkbox"/>

6.1.34	Ensure the operating system enables a user's session lock until that user re-establishes access	<input type="checkbox"/>	<input type="checkbox"/>
6.1.35	Ensure the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
6.1.36	Ensure the operating system initiates a session lock after 15 minutes of inactivity	<input type="checkbox"/>	<input type="checkbox"/>
6.1.37	Ensure all accounts on the system are assigned to an active system, application, or user account	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1	Ensure password fields are not empty	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Ensure root PATH Integrity	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Ensure no legacy "+" entries exist in /etc/shadow	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure no legacy "+" entries exist in /etc/group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure root is the only UID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure users' home directories permissions are 750 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure emergency accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
6.2.9	Ensure users own their home directories	<input type="checkbox"/>	<input type="checkbox"/>
6.2.10	Ensure users' dot files are not group or world writable	<input type="checkbox"/>	<input type="checkbox"/>
6.2.11	Ensure no users have .forward files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.12	Ensure no users have .netrc files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.13	Ensure users' .netrc Files are not group or world accessible	<input type="checkbox"/>	<input type="checkbox"/>
6.2.14	Ensure no users have .rhosts files	<input type="checkbox"/>	<input type="checkbox"/>
6.2.15	Ensure all groups in /etc/passwd exist in /etc/group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.16	Ensure no duplicate UIDs exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.17	Ensure no duplicate GIDs exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.18	Ensure no duplicate user names exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.19	Ensure no duplicate group names exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.20	Ensure shadow group is empty	<input type="checkbox"/>	<input type="checkbox"/>
6.2.21	Ensure all users' home directories exist	<input type="checkbox"/>	<input type="checkbox"/>
6.2.22	Ensure the assigned home directory of all local interactive users is group-owned by that user's primary GID	<input type="checkbox"/>	<input type="checkbox"/>
6.2.23	Ensure the assigned home directory of all local interactive users exists	<input type="checkbox"/>	<input type="checkbox"/>
6.2.24	Ensure all local interactive users are assigned a home directory upon creation	<input type="checkbox"/>	<input type="checkbox"/>
6.2.25	Ensure all local initialization files have a mode of "0740" or less permissive	<input type="checkbox"/>	<input type="checkbox"/>
6.2.26	Ensure all local files and directories have a valid owner	<input type="checkbox"/>	<input type="checkbox"/>
6.2.27	Ensure all local files and directories have a valid group	<input type="checkbox"/>	<input type="checkbox"/>
6.2.28	Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file	<input type="checkbox"/>	<input type="checkbox"/>
6.2.29	Ensure file executable search path statements do not share sensitive home directory information	<input type="checkbox"/>	<input type="checkbox"/>

6.2.30	Ensure local interactive users have a home directory assigned	<input type="checkbox"/>	<input type="checkbox"/>
6.2.31	Ensure the operating system limits the number of concurrent sessions to "10" for all accounts and/or account types	<input type="checkbox"/>	<input type="checkbox"/>
6.2.32	Ensure the operating system enables a user's session lock until that user re-establishes access	<input type="checkbox"/>	<input type="checkbox"/>
6.2.33	Ensure the operating system enables the user to initiate a session lock	<input type="checkbox"/>	<input type="checkbox"/>
6.2.34	Ensure the operating system prevents a user from overriding settings for graphical user interfaces	<input type="checkbox"/>	<input type="checkbox"/>
6.2.35	Ensure all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750"	<input type="checkbox"/>	<input type="checkbox"/>
6.2.36	Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of	<input type="checkbox"/>	<input type="checkbox"/>
6.2.37	Ensure temporary accounts have been provisioned with an expiration date of 72 hours	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure the operating system removes all software components after updated versions have been installed	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure there are no ".shosts" files on the operating system	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Ensure there are no "shosts.equiv" files on the operating system	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
15 November 2021	1.0.0	Initial Release