

CIS Ubuntu Linux 20.04 LTS STIG

v1.0.0 - 07-26-2021

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	19
Intended Audience.....	19
Consensus Guidance.....	19
Typographical Conventions	21
Assessment Status.....	21
Profile Definitions	22
Acknowledgements	24
Recommendations	25
1 Initial Setup.....	25
1.1 Filesystem Configuration	26
1.1.1 Disable unused filesystems.....	27
1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated)	28
1.1.1.2 Ensure mounting of freevxf filesystems is disabled (Automated)	30
1.1.1.3 Ensure mounting of jffs2 filesystems is disabled (Automated).....	32
1.1.1.4 Ensure mounting of hfs filesystems is disabled (Automated)	34
1.1.1.5 Ensure mounting of hfsplus filesystems is disabled (Automated).....	36
1.1.1.6 Ensure mounting of squashfs filesystems is disabled (Manual)	38
1.1.1.7 Ensure mounting of udf filesystems is disabled (Automated).....	40
1.1.2 Ensure /tmp is configured (Automated)	42
1.1.3 Ensure nodev option set on /tmp partition (Automated)	45
1.1.4 Ensure nosuid option set on /tmp partition (Automated)	47
1.1.5 Ensure noexec option set on /tmp partition (Automated)	49
1.1.6 Ensure /dev/shm is configured (Automated)	51
1.1.7 Ensure nodev option set on /dev/shm partition (Automated)	53
1.1.8 Ensure nosuid option set on /dev/shm partition (Automated)	54
1.1.9 Ensure noexec option set on /dev/shm partition (Automated)	55
1.1.10 Ensure separate partition exists for /var (Automated)	56
1.1.11 Ensure separate partition exists for /var/tmp (Automated).....	58

1.1.12 Ensure /var/tmp partition includes the nodev option (Automated)	60
1.1.13 Ensure /var/tmp partition includes the nosuid option (Automated)	62
1.1.14 Ensure /var/tmp partition includes the noexec option (Automated).....	64
1.1.15 Ensure separate partition exists for /var/log (Automated).....	66
1.1.16 Ensure separate partition exists for /var/log/audit (Automated)	68
1.1.17 Ensure separate partition exists for /home (Automated).....	70
1.1.18 Ensure /home partition includes the nodev option (Automated)	72
1.1.19 Ensure nodev option set on removable media partitions (Manual)	74
1.1.20 Ensure nosuid option set on removable media partitions (Manual)	76
1.1.21 Ensure noexec option set on removable media partitions (Manual).....	78
1.1.22 Ensure sticky bit is set on all world-writable directories (Automated)	80
1.1.23 Disable Automounting (Automated)	82
1.1.24 Disable USB Storage (Automated)	84
1.1.25 Ensure data-at-rest encryption is enabled (Manual)	86
1.1.26 Ensure data-at-rest employs cryptographic mechanisms to prevent unauthorized modification (Manual).....	89
1.1.27 Ensure data-at-rest employs cryptographic mechanisms to prevent unauthorized disclosure (Manual).....	92
1.2 Configure Software Updates	95
1.2.1 Ensure package manager repositories are configured (Manual)	96
1.2.2 Ensure GPG keys are configured (Manual)	98
1.2.3 Ensure apt is configured to prevent installation without verification of a recognized and approved digital signature (Automated)	100
1.2.4 Ensure the Advance Package Tool removes all software components after updated versions have been installed (Automated)	103
1.3 Filesystem Integrity Checking.....	105
1.3.1 Ensure AIDE is installed (Automated)	106
1.3.2 Ensure filesystem integrity is regularly checked (Automated)	108
1.3.3 Ensure System Administrator are notified of changes to the baseline configuration or anomalies (Automated).....	111
1.3.4 Ensure aide script to check file integrity is the default (Manual)	113
1.4 Secure Boot Settings	116

1.4.1 Ensure permissions on bootloader config are not overridden (Automated)	117
1.4.2 Ensure bootloader password is set (Automated).....	119
1.4.3 Ensure permissions on bootloader config are configured (Automated).....	122
1.4.4 Ensure authentication required for single user mode (Automated)	124
1.5 Additional Process Hardening	126
1.5.1 Ensure XD/NX support is enabled (Manual).....	127
1.5.2 Ensure address space layout randomization (ASLR) is enabled (Automated)	129
1.5.3 Ensure prelink is not installed (Automated).....	133
1.5.4 Ensure core dumps are restricted (Automated).....	135
1.5.5 Ensure maxlogins is 10 or less (Automated)	137
1.5.6 Ensure kdump service is not enabled (Automated)	139
1.5.7 Ensure FIPS mode is enabled (Automated)	141
1.5.8 Ensure the Ctrl-Alt-Delete key sequence is disabled (Automated)	143
1.6 Mandatory Access Control.....	145
1.6.1 Configure AppArmor	146
1.6.1.1 Ensure AppArmor is installed (Automated)	147
1.6.1.2 Ensure AppArmor is installed, enabled, and active (Automated)	148
1.6.1.3 Ensure AppArmor is enabled in the bootloader configuration (Automated)	151
1.6.1.4 Ensure all AppArmor Profiles are in enforce or complain mode (Automated).....	153
1.6.1.5 Ensure all AppArmor Profiles are enforcing (Automated)	155
1.7 Command Line Warning Banners.....	157
1.7.1 Ensure message of the day is configured properly (Automated).....	158
1.7.2 Ensure local login warning banner is configured properly (Automated)....	160
1.7.3 Ensure remote login warning banner is configured properly (Automated)	162
1.7.4 Ensure permissions on /etc/motd are configured (Automated)	164
1.7.5 Ensure permissions on /etc/issue are configured (Automated)	166
1.7.6 Ensure permissions on /etc/issue.net are configured (Automated)	168

1.8 GNOME Display Manager	170
1.8.1 Ensure GNOME Display Manager is removed (Manual)	171
1.8.2 Ensure GDM login banner is configured (Automated)	173
1.8.3 Ensure disable-user-list is enabled (Automated).....	175
1.8.4 Ensure XDCMP is not enabled (Automated).....	177
1.8.5 Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon (Manual).....	179
1.8.6 Ensure user's session lock is enabled (Automated)	183
1.8.7 Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled (Automated).....	185
1.9 Ensure updates, patches, and additional security software are installed (Manual)	187
2 Services.....	189
2.1 Special Purpose Services	190
2.1.1 Time Synchronization.....	191
2.1.1.1 Ensure time synchronization is in use (Automated)	192
2.1.1.2 Ensure systemd-timesyncd is configured (Automated).....	194
2.1.1.3 Ensure chrony is configured (Automated)	198
2.1.1.4 Ensure ntp is configured (Automated)	201
2.1.1.5 Ensure system timezone is set to UTC or GMT (Automated).....	204
2.1.1.6 Ensure system clocks are synchronized with a time server designated for the appropriate DoD network (Automated)	206
2.1.1.7 Ensure system clocks are synchronize to the authoritative time source when the time difference is greater than one second (Automated)	209
2.1.2 Ensure X Window System is not installed (Automated)	211
2.1.3 Ensure Avahi Server is not installed (Automated)	213
2.1.4 Ensure CUPS is not installed (Automated).....	215
2.1.5 Ensure DHCP Server is not installed (Automated)	217
2.1.6 Ensure LDAP server is not installed (Automated)	219
2.1.7 Ensure NFS is not installed (Automated)	221
2.1.8 Ensure DNS Server is not installed (Automated)	223
2.1.9 Ensure FTP Server is not installed (Automated)	225

2.1.10 Ensure HTTP server is not installed (Automated)	227
2.1.11 Ensure IMAP and POP3 server are not installed (Automated).....	229
2.1.12 Ensure Samba is not installed (Automated)	231
2.1.13 Ensure HTTP Proxy Server is not installed (Automated)	233
2.1.14 Ensure SNMP Server is not installed (Automated)	235
2.1.15 Ensure mail transfer agent is configured for local-only mode (Automated)	
.....	237
2.1.16 Ensure rsync service is not installed (Automated)	239
2.1.17 Ensure NIS Server is not installed (Automated)	241
2.1.18 Ensure telnetd is not installed (Automated)	243
2.1.19 Ensure rsh-server is not installed (Automated).....	245
2.1.20 Ensure Endpoint Security for Linux Threat Prevention is installed (Automated).....	247
2.2 Service Clients	249
2.2.1 Ensure NIS Client is not installed (Automated)	250
2.2.2 Ensure rsh client is not installed (Automated)	252
2.2.3 Ensure talk client is not installed (Automated)	254
2.2.4 Ensure telnet client is not installed (Automated)	256
2.2.5 Ensure LDAP client is not installed (Automated).....	258
2.2.6 Ensure RPC is not installed (Automated)	260
2.3 Ensure nonessential services are removed or masked (Manual).....	262
3 Network Configuration.....	264
3.1 Disable unused network protocols and devices.....	265
3.1.1 Disable IPv6 (Manual).....	266
3.1.2 Ensure wireless interfaces are disabled (Automated)	269
3.2 Network Parameters (Host Only)	272
3.2.1 Ensure packet redirect sending is disabled (Automated)	273
3.2.2 Ensure IP forwarding is disabled (Automated)	275
3.3 Network Parameters (Host and Router).....	278
3.3.1 Ensure source routed packets are not accepted (Automated).....	279
3.3.2 Ensure ICMP redirects are not accepted (Automated)	283

3.3.3 Ensure secure ICMP redirects are not accepted (Automated)	286
3.3.4 Ensure suspicious packets are logged (Automated)	288
3.3.5 Ensure broadcast ICMP requests are ignored (Automated)	290
3.3.6 Ensure bogus ICMP responses are ignored (Automated)	292
3.3.7 Ensure Reverse Path Filtering is enabled (Automated).....	294
3.3.8 Ensure TCP SYN Cookies is enabled (Automated)	296
3.3.9 Ensure IPv6 router advertisements are not accepted (Automated).....	298
3.4 Uncommon Network Protocols	300
3.4.1 Ensure DCCP is disabled (Automated)	301
3.4.2 Ensure SCTP is disabled (Automated)	303
3.4.3 Ensure RDS is disabled (Automated)	305
3.4.4 Ensure TIPC is disabled (Automated)	307
3.5 Firewall Configuration	309
3.5.1 Configure UncomplicatedFirewall	310
3.5.1.1 Ensure ufw is installed (Automated)	311
3.5.1.2 Ensure iptables-persistent is not installed with ufw (Automated)	313
3.5.1.3 Ensure ufw service is enabled (Automated).....	315
3.5.1.4 Ensure ufw loopback traffic is configured (Automated).....	318
3.5.1.5 Ensure ufw outbound connections are configured (Manual)	320
3.5.1.6 Ensure ufw firewall rules exist for all open ports (Manual).....	322
3.5.1.7 Ensure ufw default deny firewall policy (Automated)	325
3.5.1.8 Ensure functions, ports, protocols, and services are restricted (Manual).....	327
3.5.1.9 Ensure UFW rate-limits impacted network interfaces (Manual)	330
3.5.2 Configure nftables	333
3.5.2.1 Ensure nftables is installed (Automated)	336
3.5.2.2 Ensure ufw is uninstalled or disabled with nftables (Automated)	338
3.5.2.3 Ensure iptables are flushed with nftables (Manual).....	340
3.5.2.4 Ensure a nftables table exists (Automated)	342
3.5.2.5 Ensure nftables base chains exist (Automated)	344
3.5.2.6 Ensure nftables loopback traffic is configured (Automated)	346

3.5.2.7 Ensure nftables outbound and established connections are configured (Manual)	348
3.5.2.8 Ensure nftables default deny firewall policy (Automated)	350
3.5.2.9 Ensure nftables service is enabled (Automated)	352
3.5.2.10 Ensure nftables rules are permanent (Automated)	353
3.5.3 Configure iptables.....	356
3.5.3.1.1 Ensure iptables packages are installed (Automated)	358
3.5.3.1.2 Ensure nftables is not installed with iptables (Automated)	360
3.5.3.1.3 Ensure ufw is uninstalled or disabled with iptables (Automated).....	361
3.5.3.2.1 Ensure iptables loopback traffic is configured (Automated).....	364
3.5.3.2.2 Ensure iptables outbound and established connections are configured (Manual)	366
3.5.3.2.3 Ensure iptables default deny firewall policy (Automated)	368
3.5.3.2.4 Ensure iptables firewall rules exist for all open ports (Automated)	370
3.5.3.3.1 Ensure ip6tables loopback traffic is configured (Automated)	374
3.5.3.3.2 Ensure ip6tables outbound and established connections are configured (Manual)	376
3.5.3.3.3 Ensure ip6tables default deny firewall policy (Automated).....	379
3.5.3.3.4 Ensure ip6tables firewall rules exist for all open ports (Automated)....	382
4 Logging and Auditing	385
4.1 Configure System Accounting (auditd).....	386
4.1.1 Ensure auditing is enabled.....	387
4.1.1.1 Ensure auditd is installed (Automated).....	388
4.1.1.2 Ensure auditd service is enabled (Automated)	390
4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated).....	392
4.1.1.4 Ensure audit_backlog_limit is sufficient (Automated)	394
4.1.2 Configure Data Retention	396
4.1.2.1 Ensure audit log storage size is configured (Automated)	397
4.1.2.2 Ensure audit logs are not automatically deleted (Automated)	399
4.1.2.3 Ensure system is disabled when audit logs are full (Automated)	400

4.1.2.4 Ensure shut down by default upon audit failure (Automated)	402
4.1.2.5 Ensure sufficient storage capacity to store at least one week worth of audit records (Manual).....	404
4.1.2.6 Ensure audit event multiplexor is configured to off-load audit logs onto a different system or storage media from the system being audited (Automated).....	407
4.1.2.7 Ensure security personnel are notified when storage volume reaches 75 percent utilization (Manual).....	411
4.1.2.8 Ensure crontab scrip running to offload audit events of standalone systems (Manual)	414
4.1.3 Configure auditd rules	416
4.1.3.1 Ensure events that modify date and time information are collected (Automated).....	417
4.1.3.2 Ensure kernel module loading and unloading is collected (Automated) .	420
4.1.3.3 Ensure system administrator command executions (sudo) are collected (Automated).....	424
4.1.3.4 Ensure changes to system administration scope (sudoers) is collected (Automated).....	427
4.1.3.5 Ensure file deletion events by users are collected (Automated)	429
4.1.3.6 Ensure successful file system mounts are collected (Automated).....	433
4.1.3.7 Ensure use of privileged commands is collected (Automated)	437
4.1.3.8 Ensure unsuccessful unauthorized file access attempts are collected (Automated).....	440
4.1.3.9 Ensure discretionary access control permission modification events are collected (Automated)	445
4.1.3.10 Ensure session initiation information is collected (Automated)	450
4.1.3.11 Ensure login and logout events are collected (Automated)	453
4.1.3.12 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	456
4.1.3.13 Ensure events that modify the system's network environment are collected (Automated)	458
4.1.3.14 Ensure events that modify user/group information are collected (Automated).....	462
4.1.3.15 Ensure successful and unsuccessful uses of the su command are collected (Automated).....	465

4.1.3.16 Ensure successful and unsuccessful uses of the chfn command are collected (Automated)	467
4.1.3.17 Ensure successful and unsuccessful uses of the ssh-agent command are collected (Automated)	469
4.1.3.18 Ensure successful and unsuccessful uses of the ssh-keysign command are collected (Automated)	471
4.1.3.19 Ensure successful and unsuccessful attempts to use the setxattr system call are recorded (Automated)	473
4.1.3.20 Ensure successful and unsuccessful attempts to use the lsetxattr system call are recorded (Automated)	475
4.1.3.21 Ensure successful and unsuccessful attempts to use the fsetxattr system call are recorded (Automated)	477
4.1.3.22 Ensure successful and unsuccessful attempts to use the removexattr system call are recorded (Automated)	479
4.1.3.23 Ensure successful and unsuccessful attempts to use the fremovexattr system call are recorded (Automated)	482
4.1.3.24 Ensure successful and unsuccessful attempts to use the lremovexattr system call are recorded (Automated)	485
4.1.3.25 Ensure successful and unsuccessful uses of the open_by_handle_at system call are recorded (Automated)	488
4.1.3.26 Ensure successful and unsuccessful uses of the sudo command are recorded (Automated)	491
4.1.3.27 Ensure successful and unsuccessful attempts to use the sudoedit command are recorded (Automated)	493
4.1.3.28 Ensure successful and unsuccessful attempts to use the chsh command are recorded (Automated)	495
4.1.3.29 Ensure successful and unsuccessful attempts to use the newgrp command are recorded (Automated)	497
4.1.3.30 Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)	499
4.1.3.31 Ensure successful and unsuccessful attempts to use the apparmor_parser command are recorded (Automated)	501
4.1.3.32 Ensure successful and unsuccessful attempts to use the setfac command are recorded (Automated)	503

4.1.3.33 Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)	505
4.1.3.34 Ensure successful and unsuccessful attempts to use the passwd command are recorded (Automated)	507
4.1.3.35 Ensure successful and unsuccessful attempts to use the unix_update command are recorded (Automated)	509
4.1.3.36 Ensure successful and unsuccessful attempts to use the gpasswd command are recorded (Automated)	511
4.1.3.37 Ensure successful and unsuccessful attempts to use the chage command are recorded (Automated)	513
4.1.3.38 Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)	515
4.1.3.39 Ensure successful and unsuccessful attempts to use the crontab command are recorded (Automated)	517
4.1.3.40 Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are recorded (Automated)	519
4.1.3.41 Ensure successful and unsuccessful uses of the finit_module syscall are recorded (Automated)	521
4.1.3.42 Ensure execution of privileged functions is recorded (Automated).....	524
4.1.3.43 Ensure nonlocal administrative access events are collected (Automated)	527
4.1.3.44 Ensure successful and unsuccessful attempts to use the kmod command are recorded (Automated)	530
4.1.3.45 Ensure successful and unsuccessful attempts to use the fdisk command are recorded (Automated)	532
4.1.3.46 Ensure the audit configuration is immutable (Automated).....	534
4.1.4 Configure auditd file access	536
4.1.4.1 Ensure audit log files are not read or write-accessible by unauthorized users (Automated).....	537
4.1.4.2 Ensure only authorized users own audit log files (Automated)	539
4.1.4.3 Ensure only authorized groups ownership of audit log files (Automated)	541
4.1.4.4 Ensure the audit log directory is 0750 or more restrictive (Automated)	545

4.1.4.5 Ensure audit configuration files are 0640 or more restrictive (Automated)	547
4.1.4.6 Ensure only authorized accounts own the audit configuration files (Automated).....	549
4.1.4.7 Ensure only authorized groups own the audit configuration files (Automated).....	551
4.1.4.8 Ensure audit tools are mode of 0755 or more restrictive (Automated) ...	553
4.1.4.9 Ensure audit tools are owned by root (Automated).....	555
4.1.4.10 Ensure audit tools are group-owned by root (Automated)	557
4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)	559
4.2 Configure Logging.....	562
4.2.1 Configure rsyslog	563
4.2.1.1 Ensure rsyslog is installed (Automated)	564
4.2.1.2 Ensure rsyslog Service is enabled (Automated).....	566
4.2.1.3 Ensure logging is configured (Manual).....	568
4.2.1.4 Ensure rsyslog default file permissions configured (Automated)	570
4.2.1.5 Ensure rsyslog is configured to send logs to a remote log host (Automated)	572
4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)	575
4.2.1.7 Ensure remote access methods are monitored (Automated).....	578
4.2.2 Configure journald.....	580
4.2.2.1 Ensure journald is configured to send logs to rsyslog (Automated)	581
4.2.2.2 Ensure journald is configured to compress large log files (Automated) ..	583
4.2.2.3 Ensure journald is configured to write logfiles to persistent disk (Automated).....	585
4.2.3 Ensure logrotate is configured (Manual).....	587
4.2.4 Ensure logrotate assigns appropriate permissions (Automated).....	589
4.2.5 Ensure permissions on all logfiles are configured (Automated)	591
4.2.6 Ensure /var/log is group-owned by syslog (Automated)	593
4.2.7 Ensure /var/log is owned by root (Automated).....	595

4.2.8 Ensure /var/log/syslog is group-owned by adm (Automated).....	597
4.2.9 Ensure /var/log/syslog is owned by syslog (Automated).....	599
4.2.10 Ensure /var/log/syslog is 0640 or more restrictive (Automated).....	601
5 Access, Authentication and Authorization.....	603
5.1 Configure time-based job schedulers	604
5.1.1 Ensure cron daemon is enabled and running (Automated)	605
5.1.2 Ensure permissions on /etc/crontab are configured (Automated)	607
5.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)	609
5.1.4 Ensure permissions on /etc/cron.daily are configured (Automated).....	611
5.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated).....	613
5.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated) ...	615
5.1.7 Ensure permissions on /etc/cron.d are configured (Automated)	617
5.1.8 Ensure cron is restricted to authorized users (Automated)	619
5.1.9 Ensure at is restricted to authorized users (Automated).....	621
5.2 Configure sudo	623
5.2.1 Ensure sudo is installed (Automated)	624
5.2.2 Ensure sudo commands use pty (Automated)	626
5.2.3 Ensure sudo log file exists (Automated)	628
5.2.4 Ensure only users who need access to security functions are part of sudo group (Manual)	630
5.2.5 Ensure users must reauthenticate for privilege escalation or when changing roles (Automated)	632
5.3 Configure SSH Server.....	634
5.3.1 Ensure SSH is installed and active (Automated).....	635
5.3.2 Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	638
5.3.3 Ensure permissions on SSH private host key files are configured (Automated).....	640
5.3.4 Ensure permissions on SSH public host key files are configured (Automated)	643
5.3.5 Ensure SSH access is limited (Automated)	646
5.3.6 Ensure SSH LogLevel is appropriate (Automated)	649

5.3.7 Ensure SSH X11 forwarding is disabled (Automated).....	651
5.3.8 Ensure SSH MaxAuthTries is set to 4 or less (Automated)	653
5.3.9 Ensure SSH IgnoreRhosts is enabled (Automated)	655
5.3.10 Ensure SSH HostbasedAuthentication is disabled (Automated)	657
5.3.11 Ensure SSH root login is disabled (Automated)	659
5.3.12 Ensure SSH PermitEmptyPasswords is disabled (Automated).....	661
5.3.13 Ensure SSH PermitUserEnvironment is disabled (Automated)	663
5.3.14 Ensure only strong Ciphers are used (Automated).....	665
5.3.15 Ensure only FIPS 140-2 approved Ciphers are used (Automated)	668
5.3.16 Ensure only strong MAC algorithms are used (Automated).....	671
5.3.17 Ensure only FIPS 140-2 approved MAC algorithms are used (Automated)	675
5.3.18 Ensure only strong Key Exchange algorithms are used (Automated)	678
5.3.19 Ensure SSH Idle Timeout Interval is configured (Automated)	681
5.3.20 Ensure SSH LoginGraceTime is set to one minute or less (Automated)	684
5.3.21 Ensure SSH warning banner is configured (Automated).....	686
5.3.22 Ensure SSH PAM is enabled (Automated)	688
5.3.23 Ensure SSH AllowTcpForwarding is disabled (Automated).....	690
5.3.24 Ensure SSH MaxStartups is configured (Automated)	693
5.3.25 Ensure SSH MaxSessions is limited (Automated)	695
5.3.26 Ensure network connections associated with SSH traffic are terminated after a period of inactivity (Automated)	697
5.3.27 Ensure network connections associated with SSH traffic are terminated at the end of the session or 10 minutes of inactivity (Automated)	700
5.3.28 Ensure Standard Mandatory DoD Notice and Consent Banner displayed before granting any local or remote connection to the system (Manual)	702
5.3.29 Ensure X11UseLocalhost is enabled (Automated)	707
5.4 Configure PAM.....	709
5.4.1 Ensure password creation requirements are configured (Automated)	710
5.4.2 Ensure new and changed passwords use pwquality (Automated)	714
5.4.3 Ensure lockout for failed password attempts is configured (Automated) ..	717

5.4.4 Ensure password reuse is limited (Automated)	719
5.4.5 Ensure password hashing algorithm is SHA-512 (Automated).....	721
5.4.6 Ensure password is at least 15 characters (Automated).....	723
5.4.7 Ensure password includes at least one upper-case character (Automated)	
.....	725
5.4.8 Ensure password includes at least one lower-case character (Automated)	
.....	727
5.4.9 Ensure password includes at least one numeric character (Automated)....	729
5.4.10 Ensure password includes at least one special character (Automated)	731
5.4.11 Ensure passwords can not use dictionary words (Automated)	733
5.4.12 Ensure change of at least 8 characters when passwords are changed (Automated).....	735
5.4.13 Ensure lockout for failed password attempts until the locked account is released (Automated)	737
5.4.14 Ensure the libpam-pkcs11 package is installed (Automated)	739
5.4.15 Ensure the opensc-pkcs11 is installed (Automated).....	741
5.4.16 Ensure authenticated identity is mapped to the user or group account for PKI-based authentication (Automated)	743
5.4.17 Ensure smart card logins for multifactor authentication for local and network access (Automated)	745
5.4.18 Ensure certificates are validated by constructing a certification path to an accepted trust anchor (Automated)	748
5.4.19 Ensure Personal Identity Verification credentials are electronically verified (Automated).....	751
5.4.20 Ensure PKI local cache of revocation data (Automated)	753
5.4.21 Ensure logon delay after failed logon attempt (Automated)	755
5.4.22 Ensure PAM prohibits the use of cached authentications after one day (Automated).....	757
5.4.23 Ensure last successful account logon is displayed upon logon (Automated)	
.....	759
5.5 User Accounts and Environment	761
5.5.1 Set Shadow Password Suite Parameters	762

5.5.1.1 Ensure minimum days between password changes is configured (Automated).....	763
5.5.1.2 Ensure password expiration is 365 days or less (Automated).....	765
5.5.1.3 Ensure password expiration is 60 days or less (Automated)	767
5.5.1.4 Ensure password expiration warning days is 7 or more (Automated)....	769
5.5.1.5 Ensure inactive password lock is 30 days or less (Automated).....	771
5.5.1.6 Ensure all users last password change date is in the past (Automated) ..	773
5.5.1.7 Ensure ENCRYPT_METHOD is SHA512 (Automated)	775
5.5.1.8 Ensure root account is locked (Automated)	777
5.5.1.9 Ensure emergency accounts are removed or disabled after 72 hours (Manual)	779
5.5.1.10 Ensure immediate change to a permanent password (Manual)	781
5.5.1.11 Ensure temporary accounts expiration time of 72 hours or less (Manual)	783
5.5.2 Ensure system accounts are secured (Automated)	786
5.5.3 Ensure default group for the root account is GID 0 (Automated).....	788
5.5.4 Ensure default user umask is 027 or more restrictive (Automated).....	789
5.5.5 Ensure default user umask is 077 or more restrictive (Automated).....	794
5.5.6 Ensure default user shell timeout is 900 seconds or less (Automated)	796
5.5.7 Ensure default user shell timeout is 600 seconds or less (Automated)	799
5.5.8 Ensure vlock is installed (Automated).....	802
5.6 Ensure root login is restricted to system console (Manual)	804
5.7 Ensure access to the su command is restricted (Automated)	805
5.8 Ensure /etc/ssl/certs only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities (Automated)	807
6 System Maintenance.....	809
6.1 System File Permissions.....	810
6.1.1 Audit system file permissions (Manual)	810
6.1.2 Ensure permissions on /etc/passwd are configured (Automated)	812
6.1.3 Ensure permissions on /etc/passwd- are configured (Automated).....	813
6.1.4 Ensure permissions on /etc/group are configured (Automated).....	815

6.1.5 Ensure permissions on /etc/group- are configured (Automated)	817
6.1.6 Ensure permissions on /etc/shadow are configured (Automated)	819
6.1.7 Ensure permissions on /etc/shadow- are configured (Automated)	821
6.1.8 Ensure permissions on /etc/gshadow are configured (Automated).....	823
6.1.9 Ensure permissions on /etc/gshadow- are configured (Automated)	825
6.1.10 Ensure no world writable files exist (Automated)	827
6.1.11 Ensure no unowned files or directories exist (Automated)	829
6.1.12 Ensure no ungrouped files or directories exist (Automated)	831
6.1.13 Audit SUID executables (Manual)	833
6.1.14 Audit SGID executables (Manual)	835
6.1.15 Ensure system command files are 0755 or more restrictive (Automated)	837
6.1.16 Ensure system command files are owned by root (Automated)	839
6.1.17 Ensure system command files are group-owned by root (Automated)....	841
6.1.18 Ensure directories that contain system commands set to 0755 or more restrictive (Automated).....	843
6.1.19 Ensure directories that contain system commands are owned by root (Automated).....	845
6.1.20 Ensure directories that contain system commands are group-owned by root (Automated).....	847
6.1.21 Ensure system library files are 0755 or more restrictive (Automated)	849
6.1.22 Ensure system library files are owned by root (Automated).....	851
6.1.23 Ensure system library files are group-owned by root (Automated).....	853
6.1.24 Ensure system library directories are 0755 or more restrictive (Automated).....	855
6.1.25 Ensure system library directories are owned by root (Automated)	857
6.1.26 Ensure system library directories are group-owned by root (Automated)	859
6.2 User and Group Settings	861
6.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated) .862	
6.2.2 Ensure password fields are not empty (Automated).....	864
6.2.3 Ensure all groups in /etc/passwd exist in /etc/group (Automated)	866

6.2.4 Ensure all users' home directories exist (Automated).....	868
6.2.5 Ensure users own their home directories (Automated).....	870
6.2.6 Ensure users' home directories permissions are 750 or more restrictive (Automated).....	872
6.2.7 Ensure users' dot files are not group or world writable (Automated)	874
6.2.8 Ensure no users have .netrc files (Automated)	876
6.2.9 Ensure no users have .forward files (Automated)	879
6.2.10 Ensure no users have .rhosts files (Automated)	881
6.2.11 Ensure root is the only UID 0 account (Automated).....	883
6.2.12 Ensure root PATH Integrity (Automated)	884
6.2.13 Ensure no duplicate UIDs exist (Automated)	886
6.2.14 Ensure no duplicate GIDs exist (Automated)	888
6.2.15 Ensure no duplicate user names exist (Automated)	890
6.2.16 Ensure no duplicate group names exist (Automated)	892
6.2.17 Ensure shadow group is empty (Automated)	894
Appendix: Recommendation Summary Table	896
Appendix: Change History	911

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Ubuntu Linux 20.04 LTS systems running on x86 and x64 platforms. This guide was tested against Ubuntu Linux 20.04.2 LTS.

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.

The guidance in this document includes changes to the running system configuration. Failure to test system configuration changes in a test environment prior to implementation on a production system could lead to loss of services.

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 Ubuntu Linux on an x86 or x64 platform.

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 - Server**

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.

- **STIG - Workstation**

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 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

Bill Erickson
Dave Billing
Dominic Pace
Elliot Anderson
Ely Pinto
Fredrik Silverskär
Joy Latten
Koen Laevens
Mark Birch
Tom Pietschmann
Vineetha Hari Pai
Anurag Pal
Bradley Hieber
Thomas Sjögren
James Trigg
Kenneth Karlsson
Richard Costa
Alexander Scheel

Editor

Jonathan Lewis Christopherson
Eric Pinnell

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

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 | grep -E '(cramfs|install)'  
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
```

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 freevxfs filesystems is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `freevxfs` filesystem type is a free version of the Veritas type filesystem. This is the primary filesystem type for HP-UX operating systems.

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 freevxfs | grep -E '(freevxfs|install)'  
install /bin/true  
  
# lsmod | grep freevxfs  
  
<No output>
```

Remediation:

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

Example: `vi /etc/modprobe.d/freevxfs.conf`
and add the following line:

```
install freevxfs /bin/true
```

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

```
rmmod freevxfs
```

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 jffs2 filesystems is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `jffs2` (journaling flash filesystem 2) filesystem type is a log-structured filesystem used in flash memory devices.

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 jffs2 | grep -E '(jffs2|install)'  
install /bin/true  
  
# lsmod | grep jffs2  
  
<No output>
```

Remediation:

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

Example: `vi /etc/modprobe.d/jffs2.conf`

and add the following line:

```
install jffs2 /bin/true
```

Run the following command to unload the `jffs2` module:

```
# rmmod jffs2
```

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 hfs filesystems is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `hfs` filesystem type is a hierarchical filesystem that allows you to mount Mac OS filesystems.

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 hfs | grep -E '(hfs|install)'  
install /bin/true  
  
# lsmod | grep hfs  
  
<No output>
```

Remediation:

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

Example: `vi /etc/modprobe.d/hfs.conf`

and add the following line:

```
install hfs /bin/true
```

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

```
# rmmod hfs
```

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.	●	●	●

1.1.1.5 Ensure mounting of hfsplus filesystems is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `hfsplus` filesystem type is a hierarchical filesystem designed to replace `hfs` that allows you to mount Mac OS filesystems.

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 hfsplus | grep -E '(hfsplus|install)'  
install /bin/true  
  
# lsmod | grep hfsplus  
  
<No output>
```

Remediation:

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

Example: `vi /etc/modprobe.d/hfsplus.conf`
and add the following line:

```
install hfsplus /bin/true
```

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

```
# rmmod hfsplus
```

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.	●	●	●

1.1.1.6 Ensure mounting of squashfs filesystems is disabled (Manual)

Profile Applicability:

- Level 2 - Server
- Level 2 - 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.

Impact:

Disabling `squashfs` will prevent the use of snap. Snap is a package manager for Linux for installing Snap packages.

"Snap" application packages of software are self-contained and work across a range of Linux distributions. This is unlike traditional Linux package management approaches, like APT or RPM, which require specifically adapted packages per Linux distribution on an application update and delay therefore application deployment from developers to their software's end-user. Snaps themselves have no dependency on any external store ("App store"), can be obtained from any source and can be therefore used for upstream software deployment. When snaps are deployed on versions of Linux, the Ubuntu app store is used as default back-end, but other stores can be enabled as well.

Audit:

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

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

Remediation:

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

Example: vi /etc/modprobe.d/squashfs.conf

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.	●	●	●

1.1.1.7 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 | grep -E '(udf|install)'  
install /bin/true  
  
# lsmod | grep udf  
  
<No output>
```

Remediation:

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

Example: `vi /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

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 to tmpfs or a system partition:

```
# findmnt -n /tmp  
/tmp  tmpfs  tmpfs  rw,nosuid,nodev,noexec
```

Remediation:

Configure `/etc/fstab` as appropriate.

Example:

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

OR Run the following commands to enable systemd `/tmp` mounting:

Run the following command to create the `tmp.mount` file in the correct location:

```
# cp -v /usr/share/systemd/tmp.mount /etc/systemd/system/
```

Edit `/etc/systemd/system/tmp.mount` to configure the `/tmp` mount:

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

Run the following command to reload the systemd daemon with the updated `tmp.mount` unit file:

```
# systemctl daemon-reload
```

Run the following command to enable and start `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.

`tmpfs` can be resized using the `size={size}` parameter in `/etc/fstab` or on the Options line in the `tmp.mount` file. If we don't specify the size, it will be half the RAM. *Resize tmpfs examples:*

- `/etc/fstab`

<code>tmpfs /tmp tmpfs rw,noexec,nodev,nosuid,size=2G 0 0</code>
--

- `tmp.mount`

<code>[Mount]</code> <code>What=tmpfs</code> <code>Where=/tmp</code> <code>Type=tmpfs</code> <code>Options=mode=1777,strictatime,size=2G,noexec,nodev,nosuid</code>

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.	●	●	●

1.1.3 Ensure nodev option set on /tmp 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 `/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:

```
# findmnt -n /tmp | grep -v nodev
```

Remediation:

Edit the /etc/fstab file **OR** the /etc/systemd/system/local-fs.target.wants/tmp.mount file:

If /etc/fstab is used to mount /tmp:

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 If systemd is used to mount /tmp:

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 restart the systemd daemon:

```
# systemctl daemon-reload
```

Run the following command to restart tmp.mount

```
# systemctl restart tmp.mount
```

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

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:

If a `/tmp` partition exists, verify that the `nosuid` option is set

Run the following command and verify that nothing is returned:

```
# findmnt -n /tmp | 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
```

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

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:

If a `/tmp` partition exists, verify that the `noexec` option is set.

Run the following command and verify that nothing is returned:

```
# findmnt -n /tmp | 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
```

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>2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner</p>	●	●	●

1.1.6 Ensure /dev/shm is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

/dev/shm is a traditional shared memory concept. One program will create a memory portion, which other processes (if permitted) can access. Mounting tmpfs at /dev/shm is handled automatically by systemd.

Rationale:

Any user can upload and execute files inside the /dev/shm similar to the /tmp partition. Configuring /dev/shm allows an administrator to set the noexec option on the mount, making /dev/shm 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.

Audit:

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

```
# findmnt -n /dev/shm  
/dev/shm tmpfs tmpfs rw,nosuid,nodev,noexec
```

Remediation:

Edit /etc/fstab and add or edit the following line:

```
tmpfs      /dev/shm      tmpfs      defaults,noexec,nodev,nosuid,seclabel  0 0
```

Run the following command to remount /dev/shm:

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

Additional Information:

An entry for `/dev/shm` in `/etc/fstab` will take precedence.

`tmpfs` can be resized using the `size={size}` parameter in `/etc/fstab`. If we don't specify the size, it will be half the RAM.

Example:

<code>tmpfs /dev/shm tmpfs defaults,noexec,nodev,nosuid,size=2G 0 0</code>
--

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 nodev option set on /dev/shm 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 `/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:

Run the following command and verify that nothing is returned:

```
# findmnt -n /dev/shm | 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,nosuid,nodev,noexec /dev/shm
```

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.	●	●	●

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

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 nothing is returned:

```
# findmnt -n /dev/shm | 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,nodev,noexec /dev/shm
```

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.	●	●	●

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

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify that nothing is returned:

```
# findmnt -n /dev/shm | 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,nosuid,nodev,noexec /dev/shm
```

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	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

1.1.10 Ensure separate partition exists for /var (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

```
# findmnt /var
TARGET SOURCE      FSTYPE   OPTIONS
/var  <device>  <fstype>  rw,relatime,attr2,inode64,noquota
```

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 `auditd` is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multiuser mode.

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.	●	●	●

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

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

```
# findmnt /var/tmp
TARGET      SOURCE      FSTYPE      OPTIONS
/var/tmp    <device>   <fstype>   rw,relatime,attr2,inode64,noquota
```

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.

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.	●	●	●

1.1.12 Ensure /var/tmp partition includes the nodev option (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 `/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:

If a `/var/tmp` partition exists, verify that the `nodev` option is set.

Run the following command and verify that nothing is returned:

```
# findmnt -n /var/tmp | 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,nosuid,nodev,noexec /var/tmp
```

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.	●	●	●

1.1.13 Ensure /var/tmp partition includes the nosuid option (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

If a `/var/tmp` partition exists, verify that the `nosuid` option is set.

Run the following command and verify that nothing is returned:

```
# findmnt -n /var/tmp | 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,nodev,noexec /var/tmp
```

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 /var/tmp partition includes the noexec option (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

If a `/var/tmp` partition exists, verify that the `noexec` option is set.

Run the following command and verify that nothing is returned:

```
# findmnt -n /var/tmp | 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,nosuid,nodev,noexec /var/tmp
```

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>2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner</p>	●	●	●

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

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

```
# findmnt /var/log
TARGET      SOURCE      FSTYPE      OPTIONS
/var/log    <device>    <fstype>   rw,relatime,attr2,inode64,noquota
```

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

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	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

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

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

```
# findmnt /var/log/audit
TARGET      SOURCE   FSTYPE    OPTIONS
/var/log/audit <device> <fstype> rw,relatime,attr2,inode64,noquota
```

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.

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	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

1.1.17 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:

```
# findmnt /home
TARGET SOURCE      FSTYPE      OPTIONS
/home   <device> <fstype>  rw,relatime,attr2,inode64,noquota
```

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.	●	●	●

1.1.18 Ensure /home partition includes the nodev option (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:

If a `/home` partition exists, verify that the `nodev` option is set.

Run the following command and verify that nothing is returned:

```
# findmnt -n /home | 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	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.	●	●	●

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

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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.

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.	●	●	●

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

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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.

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.	●	●	●

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

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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.

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>2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner</p>	●	●	●

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

Profile Applicability:

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

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:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238332
Rule ID: SV-238332r654171_rule
STIG ID: UBTU-20-010411
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.	●	●	●

1.1.23 Disable Automounting (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

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:

`autofs` should be removed or disabled.

Run the following commands to verify that `autofs` is not installed or is disabled

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

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

Verify result is not "enabled".

OR run the following command to verify that `autofs` is not installed

```
# dpkg -s autofs
```

Output should include:

```
package `autofs` is not installed
```

Remediation:

Run one of the following commands:

Run the following command to disable `autofs`:

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

OR run the following command to remove `autofs`

```
# apt purge autofs
```

Additional Information:

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.

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.	●	●	●

1.1.24 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 has 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.

Note: An alternative solution to disabling the usb-storage module may be found in USBCGuard. Use of USBCGuard and construction of USB device policies should be done in alignment with site policy.

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: vi /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:

```
rmmod usb-storage
```

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.	●	●	●

1.1.25 Ensure data-at-rest encryption is enabled (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating systems handling data requiring "data at rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Rationale:

Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive and tape drive, when used for backups) within an operating system.

This requirement addresses protection of user-generated data, as well as operating system-specific configuration data. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate, in accordance with the security category and/or classification of the information.

Audit:

If there is a documented and approved reason for not having data-at-rest encryption, this requirement is Not Applicable.

Verify the Ubuntu operating system prevents unauthorized disclosure or modification of all information requiring at-rest protection by using disk encryption.

Determine the partition layout for the system with the following command:

```
# fdisk -l

(...)
Disk /dev/vda: 15 GiB, 16106127360 bytes, 31457280 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 83298450-B4E3-4B19-A9E4-7DF147A5FEFB

Device Start End Sectors Size Type
/dev/vda1 2048 4095 2048 1M BIOS boot
/dev/vda2 4096 2101247 2097152 1G Linux filesystem
/dev/vda3 2101248 31455231 29353984 14G Linux filesystem
(...)
```

Verify the system partitions are all encrypted with the following command:

```
# more /etc/crypttab
```

Every persistent disk partition present must have an entry in the file.

If any partitions other than the boot partition or pseudo file systems (such as /proc or /sys) are not listed, this is a finding.

Remediation:

To encrypt an entire partition, dedicate a partition for encryption in the partition layout.

Note: Encrypting a partition in an already-installed system is more difficult because it will need to be resized and existing partitions changed.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238335
Rule ID: SV-238335r654180_rule
STIG ID: UBTU-20-010414
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	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.			●

1.1.26 Ensure data-at-rest employs cryptographic mechanisms to prevent unauthorized modification (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must implement cryptographic mechanisms to prevent unauthorized modification of all information at rest.

Rationale:

Operating 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).

Audit:

If there is a documented and approved reason for not having data-at-rest encryption, this requirement is Not Applicable.

Verify the Ubuntu operating system prevents unauthorized disclosure or modification of all information requiring at-rest protection by using disk encryption.

Determine the partition layout for the system with the following command:

```
# fdisk -l

(...)
Disk /dev/vda: 15 GiB, 16106127360 bytes, 31457280 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 83298450-B4E3-4B19-A9E4-7DF147A5FEFB

Device Start End Sectors Size Type
/dev/vda1 2048 4095 2048 1M BIOS boot
/dev/vda2 4096 2101247 2097152 1G Linux filesystem
/dev/vda3 2101248 31455231 29353984 14G Linux filesystem
(...)
```

Verify that the system partitions are all encrypted with the following command:

```
# more /etc/crypttab
```

Every persistent disk partition present must have an entry in the file.

If any partitions other than the boot partition or pseudo file systems (such as /proc or /sys) are not listed, this is a finding.

Remediation:

To encrypt an entire partition, dedicate a partition for encryption in the partition layout.

Note: Encrypting a partition in an already-installed system is more difficult because it will need to be resized and existing partitions changed.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238365
Rule ID: SV-238365r654270_rule
STIG ID: UBTU-20-010444
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	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.			●

1.1.27 Ensure data-at-rest employs cryptographic mechanisms to prevent unauthorized disclosure (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must implement cryptographic mechanisms to prevent unauthorized disclosure of all information at rest.

Rationale:

Operating 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).

Audit:

If there is a documented and approved reason for not having data-at-rest encryption, this requirement is Not Applicable.

Verify the Ubuntu operating system prevents unauthorized disclosure or modification of all information requiring at-rest protection by using disk encryption.

Determine the partition layout for the system with the following command:

```
# fdisk -l

(...)
Disk /dev/vda: 15 GiB, 16106127360 bytes, 31457280 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 83298450-B4E3-4B19-A9E4-7DF147A5FEFB

Device Start End Sectors Size Type
/dev/vda1 2048 4095 2048 1M BIOS boot
/dev/vda2 4096 2101247 2097152 1G Linux filesystem
/dev/vda3 2101248 31455231 29353984 14G Linux filesystem
(...)
```

Verify that the system partitions are all encrypted with the following command:

```
# more /etc/crypttab
```

Every persistent disk partition present must have an entry in the file.

If any partitions other than the boot partition or pseudo file systems (such as /proc or /sys) are not listed, this is a finding.

Remediation:

To encrypt an entire partition, dedicate a partition for encryption in the partition layout.

Note: Encrypting a partition in an already-installed system is more difficult because it will need to be resized and existing partitions changed.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238366
Rule ID: SV-238366r654273_rule
STIG ID: UBTU-20-010445
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	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.			●

1.2 Configure Software Updates

Debian Family Linux distributions use apt 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 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 and verify package repositories are configured correctly:

```
# apt-cache policy
```

Remediation:

Configure your package manager repositories according to site policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>7.3 Perform Automated Operating System Patch Management</p> <p>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.</p>	●	●	●
v8	<p>7.4 Perform Automated Application Patch Management</p> <p>Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.</p>	●	●	●
v7	<p>3.4 Deploy Automated Operating System Patch Management Tools</p> <p>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.</p>	●	●	●
v7	<p>3.5 Deploy Automated Software Patch Management Tools</p> <p>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.</p>	●	●	●

1.2.2 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:

```
# apt-key list
```

Remediation:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>7.3 Perform Automated Operating System Patch Management</p> <p>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.</p>	●	●	●
v8	<p>7.4 Perform Automated Application Patch Management</p> <p>Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.</p>	●	●	●
v7	<p>3.4 Deploy Automated Operating System Patch Management Tools</p> <p>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.</p>	●	●	●
v7	<p>3.5 Deploy Automated Software Patch Management Tools</p> <p>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.</p>	●	●	●

1.2.3 Ensure apt is configured to prevent installation without verification of a recognized and approved digital signature (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system's Advance Package Tool (APT) must be configured to prevent the installation of patches, service packs, device drivers, or Ubuntu operating system components without verification they have been digitally signed using a certificate 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 ensures 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 that APT is configured to prevent the installation of patches, service packs, device drivers, or Ubuntu operating system components without verification they have been digitally signed using a certificate that is recognized and approved by the organization. Check that the "AllowUnauthenticated" variable is not set at all or is set to "false" with the following command:

```
# grep AllowUnauthenticated /etc/apt/apt.conf.d/*
/etc/apt/apt.conf.d/01-vendor-Ubuntu::APT::Get::AllowUnauthenticated "false";
```

If any of the files returned from the command with "AllowUnauthenticated" are set to "true", this is a finding.

Remediation:

Configure APT to prevent the installation of patches, service packs, device drivers, or Ubuntu operating system components without verification they have been digitally signed using a certificate that is recognized and approved by the organization.

Remove/update any APT configuration files that contain the variable "AllowUnauthenticated" to "false", or remove "AllowUnauthenticated" entirely from each file. Below is an example of setting the "AllowUnauthenticated" variable to "false":

```
APT::Get::AllowUnauthenticated "false";
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238359
Rule ID: SV-238359r654319_rule
STIG ID: UBTU-20-010438
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.</p>	●	●	●
v8	<p>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v7	<p>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.</p>	●	●	●
v7	<p>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.</p>	●	●	●

1.2.4 Ensure the Advance Package Tool removes all software components after updated versions have been installed (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The Ubuntu operating system must be configured so that Advance Package Tool (APT) removes all software components after updated versions have been installed.

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 is configured to remove all software components after updated versions have been installed with the following command:

```
# grep -i remove-unused /etc/apt/apt.conf.d/50unattended-upgrades
Unattended-Upgrade::Remove-Unused-Dependencies "true";
Unattended-Upgrade::Remove-Unused-Kernel-Packages "true";
```

If the "::Remove-Unused-Dependencies" and "::Remove-Unused-Kernel-Packages" parameters are not set to "true" or are missing or commented out, this is a finding.

Remediation:

Configure APT to remove all software components after updated versions have been installed.

Add or updated the following options to the "/etc/apt/apt.conf.d/50unattended-upgrades" file:

```
Unattended-Upgrade::Remove-Unused-Dependencies "true";
Unattended-Upgrade::Remove-Unused-Kernel-Packages "true";
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238370
Rule ID: SV-238370r654285_rule
STIG ID: UBTU-20-010449
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.	●	●	●
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.	●	●	●

1.3 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.

1.3.1 Ensure AIDE is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG - Server
- STIG - 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 commands to verify AIDE is installed:

```
# dpkg -s aide | grep -E '(Status:|not installed)'  
Status: install ok installed  
  
# dpkg -s aide-common | grep -E '(Status:|not installed)'  
Status: install ok installed
```

Remediation:

Install AIDE using the appropriate package manager or manual installation:

```
# apt install aide aide-common
```

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

Run the following commands to initialize AIDE:

```
# aideinit  
# mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db
```

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.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238371
Rule ID: SV-238371r654288_rule
STIG ID: UBTU-20-010450
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).			●

1.3.2 Ensure filesystem integrity is regularly checked (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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(--check|\$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 `aidcheck.service` and `aidcheck.timer` are enabled and `aidcheck.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/bin/aide.wrapper --config /etc/aide/aide.conf --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/bin/aide.wrapper --config /etc/aide/aide.conf --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

systemd timers, timer file `aidecheck.timer` and service file `aidecheck.service`, have been included as an optional alternative to using cron

Ubuntu advises using `/usr/bin/aide.wrapper` rather than calling `/usr/bin/aide` directly in order to protect the database and prevent conflicts

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).			●

1.3.3 Ensure System Administrator are notified of changes to the baseline configuration or anomalies (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The Ubuntu operating system must notify designated personnel if baseline configurations are changed in an unauthorized manner. The file integrity tool must notify the System Administrator when changes to the baseline configuration or anomalies

Rationale:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's IMO/ISSO and SAs must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Audit:

Verify that Advanced Intrusion Detection Environment (AIDE) notifies the System Administrator

when anomalies in the operation of any security functions are discovered with the following command:

```
# grep SILENTREPORTS /etc/default/aide  
SILENTREPORTS=no
```

If SILENTREPORTS is commented out, this is a finding.

If SILENTREPORTS is set to "yes", this is a finding.

If SILENTREPORTS is not set to "no", this is a finding.

Remediation:

Configure the Ubuntu operating system to notify designated personnel if baseline configurations are changed in an unauthorized manner.

Modify the "SILENTREPORTS" parameter in the "/etc/default/aide" file with a value of "no" if it does not already exist.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238358
Rule ID: SV-238358r654249_rule
STIG ID: UBTU-20-010437
Severity: CAT II

Vul ID: V-238372
Rule ID: SV-238372r654318_rule
STIG ID: UBTU-20-010451
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).			●

1.3.4 Ensure aide script to check file integrity is the default (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must be configured so that the script which runs each 30 days or less to check file integrity is the default one.

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.

Notifications provided by information systems include, for example, electronic alerts to System Administrators, messages to local computer consoles, and/or hardware indications, such as lights.

This requirement applies to the Ubuntu operating system performing security function verification/testing and/or systems and environments that require this functionality.

Audit:

Verify that the Advanced Intrusion Detection Environment (AIDE) default script used to check file integrity each 30 days or less is unchanged.

Download the original aide-common package in the /tmp directory:

```
# cd /tmp; apt download aide-common
```

Fetch the SHA1 of the original script file:

```
# dpkg-deb --fsys-tarfile /tmp/aide-common_*.deb | tar -xO  
./usr/share/aide/config/cron.daily/aide | shasum  
32958374f18871e3f7dda27a58d721f471843e26 -
```

Compare with the SHA1 of the file in the daily or monthly cron directory:

```
# shasum /etc/cron.{daily,monthly}/aide 2>/dev/null  
32958374f18871e3f7dda27a58d721f471843e26 /etc/cron.daily/aide
```

If there is no AIDE script file in the cron directories, or the SHA1 value of at least one file in the daily or monthly cron directory does not match the SHA1 of the original, this is a finding.

Remediation:

The cron file for AIDE is fairly complex as it creates the report. This file is installed with the "aide-common" package, and the default can be restored by copying it from the package:

Download the original package to the /tmp dir:

```
# cd /tmp; apt download aide-common
```

Extract the aide script to its original place:

```
# dpkg-deb --fsys-tarfile /tmp/aide-common_*.deb | sudo tar -x  
./usr/share/aide/config/cron.daily/aide -C /
```

Copy it to the cron.daily directory:

```
# cp -f /usr/share/aide/config/cron.daily/aide /etc/cron.daily/aide
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238236
Rule ID: SV-238236r653883_rule
STIG ID: UBTU-20-010074
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.	●	●	●

1.4 Secure Boot Settings

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

1.4.1 Ensure permissions on bootloader config are not overridden (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The permissions on /boot/grub/grub.cfg are changed to 444 when grub.cfg is updated by the update-grub command

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 command and verify the output:

```
# grep -E '^chmod\s+[0-7][0-7][0-7]\s+\${grub_cfg}\}.new' -A 1 -B1
/usr/sbin/grub-mkconfig
```

Verify the output is:

```
if [ "x${grub_cfg}" != "x" ]; then
    chmod 400 ${grub_cfg}.new || true
fi
```

Remediation:

Run the following command to update `chmod 444` to `chmod 400` in `/usr/sbin/grub-mkconfig`:

```
# sed -ri 's/chmod\s+[0-7][0-7][0-7]\s+\$\{grub_cfg\}\}.new/chmod 400
${grub_cfg}.new/' /usr/sbin/grub-mkconfig
```

Run the following command to remove check on password not being set to before running `chmod` command:

```
# sed -ri 's/ && ! grep "\^password" \${grub_cfg}.new >/dev/null//'
/usr/sbin/grub-mkconfig
```

Default Value:

```
if [ "x${grub_cfg}" != "x" ] && ! grep "\^password" ${grub_cfg}.new
>/dev/null; then
    chmod 444 ${grub_cfg}.new || true
fi
```

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.	●	●	●

1.4.2 Ensure bootloader password is set (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG - Server
- STIG - 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 AppArmor 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.

More Information: <https://help.ubuntu.com/community/Grub2/Passwords>

Audit:

Run the following commands and verify output matches:

```
# grep "^\s+set superusers" /boot/grub/grub.cfg  
set superusers=<username>  
  
# grep "^\s+password" /boot/grub/grub.cfg  
password_pbkdf2 <username> <encrypted-password>
```

Remediation:

Create an encrypted password with `grub-mkpasswd-pbkdf2`:

```
# grub-mkpasswd-pbkdf2  
  
Enter password: <password>  
Reenter password: <password>  
PBKDF2 hash of your password is <encrypted-password>
```

Add the following into a custom `/etc/grub.d` configuration file:

```
cat <<EOF  
set superusers=<username>  
password_pbkdf2 <username> <encrypted-password>  
EOF
```

The superuser/user information and password should not be contained in the `/etc/grub.d/00_header` file as this file could be overwritten in a package update.

If there is a requirement to be able to boot/reboot without entering the password, edit `/etc/grub.d/10_linux` and add `--unrestricted` to the line `CLASS=`
Example:

```
CLASS="--class gnu-linux --class gnu --class os --unrestricted"
```

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

```
# update-grub
```

Default Value:

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

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

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238204
Rule ID: SV-238204r653787_rule
STIG ID: UBTU-20-010009
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.	●	●	●

1.4.3 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.

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 command and verify `Uid` and `Gid` are both `0/root` and `Access` is `0400` or more restrictive.

```
# stat /boot/grub/grub.cfg
Access: (0400/-r-----)  Uid: (      0/    root)    Gid: (      0/    root)
```

Remediation:

Run the following commands to set permissions on your grub configuration:

```
# chown root:root /boot/grub/grub.cfg
# chmod u-wx,go-rwx /boot/grub/grub.cfg
```

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/grub/grub.cfg` with the appropriate grub configuration file 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.	●	●	●

1.4.4 Ensure authentication required for single user mode (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Single user 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 prevents an unauthorized user from rebooting the system into single user to gain root privileges without credentials.

Audit:

Perform the following to determine if a password is set for the `root` user:

```
# grep -Eq '^root:[\$0-9]' /etc/shadow || echo "root is locked"
```

No results should be returned.

Remediation:

Run the following command and follow the prompts to set a password for the `root` user:

```
# passwd 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.	●	●	●

1.5 Additional Process Hardening

1.5.1 Ensure XD/NX support is enabled (Manual)

Profile Applicability:

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

Description:

Recent processors in the x86 family support the ability to prevent code execution on a per memory page basis. Generically and on AMD processors, this ability is called No Execute (NX), while on Intel processors it is called Execute Disable (XD). This ability can help prevent exploitation of buffer overflow vulnerabilities and should be activated whenever possible. Extra steps must be taken to ensure that this protection is enabled, particularly on 32-bit x86 systems. Other processors, such as Itanium and POWER, have included such support since inception and the standard kernel for those platforms supports the feature.

Note: Ensure your system supports the XD or NX bit and has PAE support before implementing this recommendation as this may prevent it from booting if these are not supported by your hardware

Rationale:

Enabling any feature that can protect against buffer overflow attacks enhances the security of the system.

Audit:

Run the following command and verify your kernel has identified and activated NX/XD protection.

```
# journalctl | grep 'protection: active'  
kernel: NX (Execute Disable) protection: active
```

OR on systems without journalctl:

```
# [[ -n $(grep noexec[0-9]*=off /proc/cmdline) || -z $(grep -E -i ' (pae|nx)' /proc/cpuinfo) || -n $(grep '\sNX\s.*\sprotection:\s' /var/log/dmesg | grep -v active) ]] && echo "NX Protection is not active"
```

Nothing should be returned

Remediation:

On 32 bit systems install a kernel with PAE support, no installation is required on 64 bit systems:

If necessary configure your bootloader to load the new kernel and reboot the system.

You may need to enable NX or XD support in your bios.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238368
Rule ID: SV-238368r654279_rule
STIG ID: UBTU-20-010447
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.		●	●

1.5.2 Ensure address space layout randomization (ASLR) is enabled (Automated)

Profile Applicability:

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

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 -Es "\s*kernel\.randomize_va_space\s*=\s*([0-1]| [3-9]| [1-9] [0-9]+)"  
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf  
/usr/local/lib/sysctl.d/*.conf /run/sysctl.d/*.conf  
  
Nothing should be returned
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file ending in `.conf`:

```
kernel.randomize_va_space = 2
```

Run the following script to comment out entries that override the default setting of `kernel.randomize_va_space`:

```
#!/usr/bin/bash

for file in /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /run/sysctl.d/*.conf; do
    if [ -f "$file" ]; then
        grep -Esq "^\s*kernel\.randomize_va_space\s*=\s*([0-1]|[3-9]|[1-9][0-9]+)" "$file" && sed -ri 's/^\s*kernel\.randomize_va_space\s*=\s*([0-1]|[3-9]|[1-9][0-9]+)/#/ &/gi' "$file"
    fi
done
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.randomize_va_space=2
```

Default Value:

`kernel.randomize_va_space = 2`

References:

1. <http://manpages.ubuntu.com/manpages/focal/man5/sysctl.d.5.html>

Additional Information:

Configuration files are read from directories in `/etc/`, `/run/`, `/usr/local/lib/`, and `/lib/`, in order of precedence. Files must have the ".conf" extension. Files in `/etc/` override files with the same name in `/run/`, `/usr/local/lib/`, and `/lib/`. Files in `/run/` override files with the same name under `/usr/`.

All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Thus, the configuration in a certain file may either be replaced completely (by placing a file with the same name in a directory with higher priority), or individual settings might be changed (by specifying additional settings in a file with a different name that is ordered later).

Packages should install their configuration files in `/usr/lib/` (distribution packages) or `/usr/local/lib/` (local installs). Files in `/etc/` are reserved for the local administrator, who may use this logic to override the configuration files installed by vendor packages. It is recommended to prefix all filenames with a two-digit number and a dash, to simplify the ordering of the files.

If the administrator wants to disable a configuration file supplied by the vendor, the recommended way is to place a symlink to `/dev/null` in the configuration directory in `/etc/`, with the same filename as the vendor configuration file. If the vendor configuration file is included in the initrd image, the image has to be regenerated.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238369
Rule ID: SV-238369r654282_rule
STIG ID: UBTU-20-010448
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> 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 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> 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.		●	●

1.5.3 Ensure prelink is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`prelink` is a program that modifies ELF shared libraries and ELF dynamically linked binaries in such a way that the time needed for the dynamic linker to perform relocations at startup significantly decreases.

Rationale:

The prelinking feature can interfere with the operation of AIDE, because it changes binaries. Prelinking can also increase the vulnerability of the system if a malicious user is able to compromise a common library such as `libc`.

Audit:

Verify `prelink` is not installed:

```
# dpkg -s prelink | grep -E '(Status:|not installed)'  
dpkg-query: package 'prelink' is not installed and no information is  
available
```

Remediation:

Run the following command to restore binaries to normal:

```
# prelink -ua
```

Uninstall `prelink` using the appropriate package manager or manual installation:

```
# apt purge prelink
```

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>14.9 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).</p>			●

1.5.4 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 -Es '^(\*|\s).*hard.*core.*(\s+\#.*)?$' /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`, `masked`, 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.	●	●	●

1.5.5 Ensure maxlogins is 10 or less (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must limit the number of concurrent sessions to ten for all accounts and/or account types.

Rationale:

The Ubuntu 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 upon mission needs and the operational environment for each system.

Audit:

Verify the Ubuntu operating system limits the number of concurrent sessions to 10 for all accounts and/or account types by running the following command:

```
# grep maxlogins /etc/security/limits.conf | grep -v '^* hard maxlogins'
```

The result must contain the following line:

- hard maxlogins 10

If the "maxlogins" item is missing or the value is not set to 10 or less or is commented out, this is a finding.

Remediation:

Configure the Ubuntu 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" file:

```
* hard maxlogins 10
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238323

Rule ID: SV-238323r654144_rule

STIG ID: UBTU-20-010400

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.	●	●	●

1.5.6 Ensure kdump service is not enabled (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must disable kernel core dumps so that it can fail to a secure state if system initialization fails, shutdown fails or aborts fail.

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.

Audit:

Verify that kernel core dumps are disabled unless needed.

Check if "kdump" service is active with the following command:

```
# systemctl is-active kdump.service  
inactive
```

If the "kdump" service is active, ask the SA if the use of the service is required and documented with the 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:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238334
Rule ID: SV-238334r654177_rule
STIG ID: UBTU-20-010413
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.		●	●

1.5.7 Ensure FIPS mode is enabled (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must implement NIST FIPS-validated cryptography to protect classified information and for the following: to provision digital signatures, to generate cryptographic hashes, and to protect unclassified information requiring confidentiality and cryptographic protection 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 utilizing 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.

Satisfies: SRG-OS-000396-GPOS-00176, SRG-OS-000478-GPOS-00223

Impact:

Enabling a FIPS mode on a pre-existing system involves a number of modifications to the Ubuntu operating system. Refer to the Ubuntu Server 18.04 FIPS 140-2 security policy document for instructions.

Note: A subscription to the "Ubuntu Advantage" plan is required in order to obtain the FIPS Kernel cryptographic modules and enable FIPS.

Audit:

Verify the system is configured to run in FIPS mode with the following command:

```
# grep -i 1 /proc/sys/crypto/fips_enabled  
1
```

If a value of "1" is not returned, this is a finding.

Remediation:

Configure the system to run in FIPS mode. Add "fips=1" to the kernel parameter during the Ubuntu operating systems install.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238363
Rule ID: SV-238363r654320_rule
STIG ID: UBTU-20-010442
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.	●	●	●

1.5.8 Ensure the Ctrl-Alt-Delete key sequence is disabled (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must disable the x86 Ctrl-Alt-Delete key sequence.

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.

Audit:

Verify the Ubuntu operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed.

Check that the "ctrl-alt-del.target" (otherwise also known as reboot.target) is not active with the following command:

```
# systemctl status ctrl-alt-del.target  
  
reboot.target - Reboot  
Loaded: loaded (/usr/lib/systemd/system/reboot.target; disabled)  
Active: inactive (dead)  
Docs: man:systemd.special(7)
```

If the "ctrl-alt-del.target" is active, this is a finding.

Remediation:

Configure the system to disable the Ctrl-Alt-Delete sequence for the command line with the following command:

```
# sudo systemctl mask ctrl-alt-del.target
```

Reload the daemon to take effect:

```
# sudo systemctl daemon-reload
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238380
Rule ID: SV-238380r654315_rule
STIG ID: UBTU-20-010460
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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.6 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.

Notes:

- *Apparmor is the default MAC provided with Debian systems.*
- *Additional Mandatory Access Control systems to include SELinux exist. If a different Mandatory Access Control systems is used, please follow it's vendors guidance for proper implementation in place of the guidance provided in this section*

1.6.1 Configure AppArmor

AppArmor provides a Mandatory Access Control (MAC) system that greatly augments the default Discretionary Access Control (DAC) model. Under AppArmor MAC rules are applied by file paths instead of by security contexts as in other MAC systems. As such it does not require support in the filesystem and can be applied to network mounted filesystems for example. AppArmor security policies define what system resources applications can access and what privileges they can do so with. 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 AppArmor MAC rules. The action will not be allowed if either one of these models does not permit the action. In this way, AppArmor rules can only make a system's permissions more restrictive and secure.

References:

1. AppArmor Documentation: <http://wiki.apparmor.net/index.php/Documentation>
2. Ubuntu AppArmor Documentation:
<https://help.ubuntu.com/community/AppArmor>
3. SUSE AppArmor Documentation:
<https://www.suse.com/documentation/apparmor/>

1.6.1.1 Ensure AppArmor is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

AppArmor provides Mandatory Access Controls.

Rationale:

Without a Mandatory Access Control system installed only the default Discretionary Access Control system will be available.

Audit:

Verify that AppArmor is installed:

```
# dpkg -s apparmor | grep -E '(Status:|not installed)'  
Status: install ok installed
```

Remediation:

Install AppArmor.

```
# apt install apparmor
```

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.	●	●	●

1.6.1.2 Ensure AppArmor is installed, enabled, and active (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The Ubuntu operating system must be configured to use AppArmor.

Rationale:

Control of program execution is a mechanism used to prevent execution of unauthorized programs. Some operating systems may provide a capability that runs counter to the mission or provides users with functionality that exceeds mission requirements. This includes functions and services installed at the operating system-level.

Some of the programs, installed by default, may be harmful or may not be necessary to support essential organizational operations (e.g., key missions, functions). Removal of executable programs is not always possible; therefore, establishing a method of preventing program execution is critical to maintaining a secure system baseline.

Methods for complying with this requirement include restricting execution of programs in certain environments, while preventing execution in other environments; or limiting execution of certain program functionality based on organization-defined criteria (e.g., privileges, subnets, sandboxed environments, or roles).

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000312-GPOS-00122, SRG-OS-000312-GPOS-00123, SRG-OS-000312-GPOS-00124, SRG-OS-000324-GPOS-00125, SRG-OS-000370-GPOS-00155

Audit:

Verify the operating system prevents program execution in accordance with local policies.

Check that AppArmor is installed and active by running the following command,

```
$ dpkg -l | grep apparmor
```

If the "apparmor" package is not installed, this is a finding.

```
$ systemctl is-active apparmor.service
```

active

If "active" is not returned, this is a finding.

```
$ systemctl is-enabled apparmor.service
```

enabled

If "enabled" is not returned, this is a finding.

Remediation:

Install "AppArmor" (if it is not installed) with the following command:

```
# apt-get install apparmor  
# systemctl enable apparmor.service
```

Start "apparmor" with the following command:

```
# systemctl start apparmor.service
```

Note: AppArmor must have properly configured profiles for applications and home directories. All configurations will be based on the actual system setup and organization and normally are on a per role basis. See the AppArmor documentation for more information on configuring profiles.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238360

Rule ID: SV-238360r654255_rule

STIG ID: UBTU-20-010439

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.7 Enforce Access Control to Data through Automated Tools Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			●

1.6.1.3 Ensure AppArmor is enabled in the bootloader configuration (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure AppArmor to be enabled at boot time and verify that it has not been overwritten by the bootloader boot parameters.

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

Rationale:

AppArmor must be enabled at boot time in your bootloader configuration to ensure that the controls it provides are not overridden.

Audit:

Run the following commands to verify that all `linux` lines have the `apparmor=1` and `security=apparmor` parameters set:

```
# grep "^\s*linux" /boot/grub/grub.cfg | grep -v "apparmor=1"  
Nothing should be returned  
  
# grep "^\s*linux" /boot/grub/grub.cfg | grep -v "security=apparmor"  
Nothing should be returned
```

Remediation:

Edit `/etc/default/grub` and add the `apparmor=1` and `security=apparmor` parameters to the `GRUB_CMDLINE_LINUX`= line

```
GRUB_CMDLINE_LINUX="apparmor=1 security=apparmor"
```

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

```
# update-grub
```

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.	●	●	●

1.6.1.4 Ensure all AppArmor Profiles are in enforce or complain mode (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

AppArmor profiles define what resources applications are able to access.

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 any policies that exist on the system are activated.

Audit:

Run the following command and verify that profiles are loaded, and are in either enforce or complain mode:

```
# apparmor_status | grep profiles
```

Review output and ensure that profiles are loaded, and in either enforce or complain mode:

```
37 profiles are loaded.  
35 profiles are in enforce mode.  
2 profiles are in complain mode.  
4 processes have profiles defined.
```

Run the following command and verify no processes are unconfined

```
# apparmor_status | grep processes
```

Review the output and ensure no processes are unconfined:

```
4 processes have profiles defined.  
4 processes are in enforce mode.  
0 processes are in complain mode.  
0 processes are unconfined but have a profile defined.
```

Remediation:

Run the following command to set all profiles to enforce mode:

```
# aa-enforce /etc/apparmor.d/*
```

OR

Run the following command to set all profiles to complain mode:

```
# aa-complain /etc/apparmor.d/*
```

Note: Any unconfined processes may need to have a profile created or activated for them and then be restarted

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.	●	●	●

1.6.1.5 Ensure all AppArmor Profiles are enforcing (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

AppArmor profiles define what resources applications are able to access.

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 any policies that exist on the system are activated.

Audit:

Run the following commands and verify that profiles are loaded and are not in complain mode:

```
# apparmor_status | grep profiles
```

Review output and ensure that profiles are loaded, and in enforce mode:

```
34 profiles are loaded.  
34 profiles are in enforce mode.  
0 profiles are in complain mode.  
2 processes have profiles defined.
```

Run the following command and verify that no processes are unconfined:

```
apparmor_status | grep processes
```

Review the output and ensure no processes are unconfined:

```
2 processes have profiles defined.  
2 processes are in enforce mode.  
0 processes are in complain mode.  
0 processes are unconfined but have a profile defined.
```

Remediation:

Run the following command to set all profiles to enforce mode:

```
# aa-enforce /etc/apparmor.d/*
```

Note: Any unconfined processes may need to have a profile created or activated for them and then be restarted

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 Command Line Warning Banners

Presenting a warning message prior to the normal user login may assist in the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific exploits at a system. The `/etc/motd`, `/etc/issue`, and `/etc/issue.net` files govern warning banners for standard command line logins for both local and remote users.

Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. It is important that the organization's legal counsel review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific. More information (including citations of relevant case law) can be found at <http://www.justice.gov/criminal/cybercrime/>

Note: The text provided in the remediation actions for these items is intended as an example only. Please edit to include the specific text for your organization as approved by your legal department

1.7.1 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 no results are returned:

```
# grep -Eis "(\\\\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.	●	●	●

1.7.2 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.	●	●	●

1.7.3 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	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.	●	●	●

1.7.4 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`, or the file doesn't exist.

```
# stat -L /etc/motd
Access: (0644/-rw-r--r--)  Uid: (      0/    root)  Gid: (      0/    root)
OR
stat: cannot stat '/etc/motd': No such file or directory
```

Remediation:

Run the following commands to set permissions on `/etc/motd`:

```
# chown root:root $(readlink -e /etc/motd)
# chmod u-x,go-wx $(readlink -e /etc/motd)
```

OR run the following command to remove the `/etc/motd` file:

```
# rm /etc/motd
```

Default Value:

File doesn't exist

Additional Information:

If Message of the day is not needed, this file can be removed.

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.	●	●	●

1.7.5 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 -L /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 $(readlink -e /etc/issue)
# chmod u-x,go-wx $(readlink -e /etc/issue)
```

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.7.6 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 -L /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 $(readlink -e /etc/issue.net)
# chmod u-x,go-wx $(readlink -e /etc/issue.net)
```

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.8 GNOME Display Manager

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

Note: If GDM is not installed on the system, this section can be skipped

1.8.1 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 Graphical User Interface (GUI) from the system.

Audit:

Run the following command and verify `gdm3` is not installed:

```
# dpkg -s gdm3 | grep -E '(Status:|not installed)'  
dpkg-query: package 'gdm3' is not installed and no information is available
```

Remediation:

Run the following command to uninstall `gdm3`:

```
# apt purge gdm3
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

1.8.2 Ensure GDM login banner is configured (Automated)

Profile Applicability:

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

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.

Audit:

If GDM is installed on the system verify that `/etc/gdm3/greeter.dconf-defaults` file exists and contains the following:

```
[org/gnome/login-screen]
banner-message-enable=true
banner-message-text='<banner message>'
```

Remediation:

Edit or create the file `/etc/gdm3/greeter.dconf-defaults` and add the following:

```
[org/gnome/login-screen]
banner-message-enable=true
banner-message-text='<banner message>'
disable-user-list=true
```

Example banner message: 'Authorized uses only. All activity may be monitored and reported.'

Run the following command to re-load GDM on the next login or reboot:

```
# dpkg-reconfigure gdm3
```

Additional Information:

Additional options and sections may appear in the /etc/dconf/db/gdm.d/01-banner-message file.

If a different GUI login service is in use, consult your documentation and apply an equivalent banner.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238197
Rule ID: SV-238197r653766_rule
STIG ID: UBTU-20-010002
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.	●	●	●

1.8.3 Ensure disable-user-list is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

The `disable-user-list` option controls if a list of users is displayed on the login screen

Rationale:

Displaying the user list eliminates half of the Userid/Password equation that an unauthorized person would need to log on.

Audit:

Run the following command to verify that `disable-user-list` is enabled:

```
# grep -E '^s*disable-user-list\s*=\\s*true\\b'  
disable-user-list=true
```

Remediation:

Edit or create the file `/etc/gdm3/greeter.dconf-defaults` and edit or add the following:

```
[org/gnome/login-screen]  
banner-message-enable=true  
banner-message-text='<banner message>'  
disable-user-list=true
```

Run the following command to re-load GDM on the next login or reboot:

```
# dpkg-reconfigure gdm3
```

Default Value:

false

Additional Information:

If a different GUI login service is in use and required on the system, consult your documentation to disable displaying the user list

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 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/gdm3/custom.conf
```

Nothing should be returned

Remediation:

Edit the file /etc/gdm3/custom.conf and remove the line:

```
Enable=true
```

Default Value:

false (This is denoted by no Enabled= entry in the file /etc/gdm3/custom.conf in the [xdmcp] section)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

1.8.5 Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

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.\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."

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.	●	●	●

1.8.6 Ensure user's session lock is enabled (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must retain a user's session lock until that user reestablishes access using established identification and authentication procedures.

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.

Audit:

Verify the Ubuntu operation system has a graphical user interface session lock enabled.

Note: If the Ubuntu operating system does not have a graphical user interface installed, this requirement is Not Applicable.

Get the "lock-enabled" setting to verify the graphical user interface session has the lock enabled with the following command:

```
# gsettings get org.gnome.desktop.screensaver lock-enabled  
true
```

If "lock-enabled" is not set to "true", this is a finding.

Remediation:

Configure the Ubuntu operating system to allow a user to lock the current graphical user interface session.

Note: If the Ubuntu operating system does not have a graphical user interface installed, this requirement is Not Applicable.

Set the "lock-enabled" setting to allow graphical user interface session locks with the following command:

```
# gsettings set org.gnome.desktop.screensaver lock-enabled true
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238199
Rule ID: SV-238199r653772_rule
STIG ID: UBTU-20-010004
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	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

1.8.7 Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must disable the x86 Ctrl-Alt-Delete key sequence 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 the graphical 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 Ubuntu operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface.

Check that the "logout" target is not bound to an action with the following command:

```
# 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 the graphical user interface:

```
[org/gnome/settings-daemon/plugins/media-keys]
logout=''
```

Update the dconf settings:

```
# dconf update
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238379
Rule ID: SV-238379r654312_rule
STIG ID: UBTU-20-010459
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 Ensure updates, patches, and additional security software are installed (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify there are no updates or patches to install:

```
# apt -s upgrade
```

Remediation:

Run the following command to update all packages following local site policy guidance on applying updates and patches:

```
# apt upgrade
```

OR

```
# apt dist-upgrade
```

Additional Information:

Site policy may mandate a testing period before install onto production systems for available updates.

- upgrade - is used to install the newest versions of all packages currently installed on the system from the sources enumerated in /etc/apt/sources.list. Packages currently installed with new versions available are retrieved and upgraded; under no circumstances are currently installed packages removed, or packages not already installed retrieved and installed. New versions of currently installed packages that cannot be upgraded without changing the install status of another package will be left at their current version. An update must be performed first so that apt knows that new versions of packages are available.
- dist-upgrade - in addition to performing the function of upgrade, also intelligently handles changing dependencies with new versions of packages; apt has a "smart" conflict resolution system, and it will attempt to upgrade the most important packages at the expense of less important ones if necessary. So, dist-upgrade command may remove some packages. The /etc/apt/sources.list file contains a list of locations from which to retrieve desired package files. See also apt_preferences(5) for a mechanism for overriding the general settings for individual packages.

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.	●	●	●

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.

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

2.1 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 deleted from the system to reduce the potential attack surface. If a package is required as a dependency, and the service is not required, the service should be stopped and masked.

The following command can be used to stop and mask the service:

```
# systemctl --now mask <service_name>
```

2.1.1 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 a service such as `systemd-timesyncd`, `chrony`, or `ntp`.

Notes:

- *If access to a physical host's clock is available and configured according to site policy, this section can be skipped*
- *Only one time synchronization method should be in use on the system*
- *Only the section related to the time synchronization method in use on the system should be followed, all other time synchronization recommendations should be skipped*
- *If access to a physical host's clock is available and configured according to site policy, `systemd-timesyncd` should be stopped and masked*

2.1.1.1 Ensure time synchronization is in use (Automated)

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.

Notes:

- *If access to a physical host's clock is available and configured according to site policy, this section can be skipped*
- *Only one time synchronization method should be in use on the system*
- *If access to a physical host's clock is available and configured according to site policy, systemd-timesyncd should be stopped and masked*

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 timesyncd, chrony, or NTP is installed. Use one of the following commands to determine the needed information:

If systemd-timesyncd is used:

```
# systemctl is-enabled systemd-timesyncd
```

If chrony is used:

```
# dpkg -s chrony
```

If ntp is used:

```
# dpkg -s ntp
```

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 systems where host based time synchronization is not available, configure systemd-timesyncd. If "full featured" and/or encrypted time synchronization is required, install chrony or NTP.

To install chrony:

```
# apt install chrony
```

To install ntp:

```
# apt install ntp
```

On virtual systems where host based time synchronization is available consult your virtualization software documentation and setup host based synchronization

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.		●	●

2.1.1.2 Ensure systemd-timesyncd is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network. It implements an SNTP client. In contrast to NTP implementations such as chrony or the NTP reference server this only implements a client side, and does not bother with the full NTP complexity, focusing only on querying time from one remote server and synchronizing the local clock to it. The daemon runs with minimal privileges, and has been hooked up with networkd to only operate when network connectivity is available. The daemon saves the current clock to disk every time a new NTP sync has been acquired, and uses this to possibly correct the system clock early at bootup, in order to accommodate for systems that lack an RTC such as the Raspberry Pi and embedded devices, and make sure that time monotonically progresses on these systems, even if it is not always correct. To make use of this daemon a new system user and group "systemd-timesync" needs to be created on installation of systemd.

Note:

- If `chrony` or `ntp` are used, `systemd-timesyncd` should be stopped and masked, and this section skipped
- This recommendation only applies if `timesyncd` is in use on the system
- Only one time synchronization method should be in use on the system

Rationale:

Proper configuration is vital to ensuring time synchronization is working properly.

Audit:

- Verify that only one time synchronization method is in use on the system:

Run the following command to verify that `ntp` is not installed:

```
dpkg -s ntp  
dpkg-query: package 'ntp' is not installed and no information is available
```

Run the following command to verify that `chrony` is not installed:

```
dpkg -s chrony  
dpkg-query: package 'chrony' is not installed and no information is available
```

- Ensure that `timesyncd` is enabled and started

Run the following commands:

```
# systemctl is-enabled systemd-timesyncd.service  
enabled
```

- Verify that `systemd-timesyncd` is configured:

Review `/etc/systemd/timesyncd.conf` and ensure that the NTP servers, NTP FallbackNTP servers, and RootDistanceMaxSec listed are in accordance with local policy

Run the following command

```
# timedatectl status
```

This should return something similar to:

```
Local time: Tue 2019-06-04 15:40:45 EDT  
Universal time: Tue 2019-06-04 19:40:45 UTC  
RTC time: Tue 2019-06-04 19:40:45  
Time zone: America/New_York (EDT, -0400)  
NTP enabled: yes  
NTP synchronized: yes  
RTC in local TZ: no  
DST active: yes  
Last DST change: DST began at  
                  Sun 2019-03-10 01:59:59 EST  
                  Sun 2019-03-10 03:00:00 EDT  
Next DST change: DST ends (the clock jumps one hour backwards) at  
                  Sun 2019-11-03 01:59:59 EDT  
                  Sun 2019-11-03 01:00:00 EST
```

Remediation:

- Remove additional time synchronization methods:

Run the following commands to remove `ntp` and `chrony`:

```
# apt purge ntp  
# apt purge chrony
```

- Configure `systemd-timesyncd`:

Run the following command to enable `systemd-timesyncd`

```
# systemctl enable systemd-timesyncd.service
```

Edit the file `/etc/systemd/timesyncd.conf` and add/modify the following lines:

```
NTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org #Servers listed should be In  
Accordence With Local Policy  
  
FallbackNTP=2.debian.pool.ntp.org 3.debian.pool.ntp.org #Servers listed  
should be In Accordence With Local Policy  
  
RootDistanceMax=1 #should be In Accordence With Local Policy
```

Run the following commands to start `systemd-timesyncd.service`

```
# systemctl start systemd-timesyncd.service  
  
# timedatectl set-ntp true
```

Additional Information:

The `systemd-timesyncd` service specifically implements only SNTP. This minimalistic service will set the system clock for large offsets or slowly adjust it for smaller deltas. More complex use cases are not covered by `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.		●	●

2.1.1.3 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.

Notes:

- *If ntp or systemd-timesyncd are used, chrony should be removed and this section skipped*
- *This recommendation only applies if chrony is in use on the system*
- *Only one time synchronization method should be in use on the system*

Rationale:

If `chrony` is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

Audit:

Verify that only one time synchronization method is in use on the system:

Run the following command to verify that ntp is not installed:

```
dpkg -s ntp | grep -E '(Status:|not installed)'  
dpkg-query: package 'ntp' is not installed and no information is available
```

Run the following command to verify that systemd-timesyncd is masked:

```
# systemctl is-enabled systemd-timesyncd  
masked
```

Verify that chrony is configured:

Run the following command and verify remote server is configured properly:

```
# grep -E "^(server|pool)" /etc/chrony/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
```

Note: The compiled-in default value is _chrony

Remediation:

Remove and/or disable additional time synchronization methods:

Run the following command to remove ntp:

```
# apt purge ntp
```

Run the following command to stop and mask systemd-timesyncd:

```
# systemctl --now mask systemd-timesyncd
```

Configure chrony:

Add or edit server or pool lines to /etc/chrony/chrony.conf as appropriate:

```
server <remote-server>
```

Add or edit the user line to /etc/chrony/chrony.conf:

```
user _chrony
```

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.		●	●

2.1.1.4 Ensure ntp is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`ntp` is a daemon which implements the Network Time Protocol (NTP). It is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on NTP can be found at <http://www.ntp.org>. `ntp` can be configured to be a client and/or a server.

Notes:

- *If chrony or systemd-timesyncd are used, ntp should be removed and this section skipped*
- *This recommendation only applies if ntp is in use on the system*
- *Only one time synchronization method should be in use on the system*

Rationale:

If `ntp` is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

Audit:

- Verify that only one time synchronization method is in use on the system:

Run the following command to verify `chrony` is not in use on the system:

```
# dpkg -s chrony | grep -E '(Status:|not installed)'  
dpkg-query: package 'chrony' is not installed and no information is available
```

Run the following command to verify that `systemd-timesyncd` is not in use on the system:

```
# systemctl is-enabled systemd-timesyncd  
masked
```

- Verify that `ntp` is configured:

Run the following command and verify output matches:

```
# grep '^restrict' /etc/ntp.conf  
restrict -4 default kod nomodify notrap nopeer noquery  
restrict -6 default kod nomodify notrap nopeer noquery
```

The `-4` in the first line is optional and options after `default` can appear in any order.

Additional restriction lines may exist

Run the following command and verify remote server is configured properly:

```
# grep -E "^(server|pool)" /etc/ntp.conf  
server <remote-server>
```

Multiple servers may be configured.

Verify that `ntp` is configured to run as the `ntp` user by running the following command and verifying output matches:

```
# grep "RUNASUSER=ntp" /etc/init.d/ntp  
RUNASUSER=ntp
```

Additional options may be present

Remediation:

- Remove and/or disable additional time synchronization methods:

Run the following command to remove `chrony`:

```
apt purge chrony
```

Run the following command to stop and mask `systemd-timesyncd`:

```
# systemctl --now mask systemd-timesyncd
```

- Configure `ntp`:

Add or edit restrict lines in `/etc/ntp.conf` to match the following:

```
restrict -4 default kod nomodify notrap nopeer noquery  
restrict -6 default kod nomodify notrap nopeer noquery
```

Add or edit server or pool lines to `/etc/ntp.conf` as appropriate:

```
server <remote-server>
```

Configure `ntp` to run as the `ntp` user by adding or editing the `/etc/init.d/ntp` file:

```
RUNASUSER=ntp
```

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.		●	●

2.1.1.5 Ensure system timezone is set to UTC or GMT (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The Ubuntu operating system must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

Rationale:

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.

Audit:

To verify the time zone is configured to use UTC or GMT, run the following command.

```
# timedatectl status | grep -i "time zone"  
Timezone: UTC (UTC, +0000)
```

If "Timezone" is not set to UTC or GMT, this is a finding.

Remediation:

To configure the system time zone to use UTC or GMT, run the following command, replacing [ZONE] with UTC or GMT:

```
# timedatectl set-timezone [ZONE]
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238308
Rule ID: SV-238308r654099_rule
STIG ID: UBTU-20-010230
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.	●	●	●

2.1.1.6 Ensure system clocks are synchronized with a time server designated for the appropriate DoD network (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must, for networked systems, compare internal information system clocks at least every 24 hours with a server which is synchronized to one of the redundant 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).

Audit:

If the system is not networked, this requirement is Not Applicable.

The system clock must be configured to compare the system clock at least every 24 hours to the authoritative time source.

Check the value of "maxpoll" in the "/etc/chrony/chrony.conf" file with the following command:

```
$ sudo grep maxpoll /etc/chrony/chrony.conf  
server tick.usno.navy.mil iburst maxpoll 17
```

If "maxpoll" is not set to "17" or does not exist, this is a finding.

Verify that the "chrony.conf" file is configured to an authoritative DoD time source by running the following command:

```
# grep -i server /etc/chrony/chrony.conf  
  
server tick.usno.navy.mil iburst maxpoll 17  
server tock.usno.navy.mil iburst maxpoll 17  
server ntp2.usno.navy.mil iburst maxpoll 17
```

If the parameter "server" is not set, is not set to an authoritative DoD time source, or is commented out, this is a finding.

Remediation:

If the system is not networked, this requirement is Not Applicable.

To configure the system clock to compare the system clock at least every 24 hours to the authoritative time source, edit the "/etc/chrony/chrony.conf" file. Add or correct the following lines, by replacing "[source]" in the following line with an authoritative DoD time source:

```
server [source] iburst maxpoll = 17
```

If the "chrony" service was running and the value of "maxpoll" or "server" was updated, the service must be restarted using the following command:

```
# systemctl restart chrony.service
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238356
Rule ID: SV-238356r654317_rule
STIG ID: UBTU-20-010435
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.		●	●

**2.1.1.7 Ensure system clocks are synchronize to the authoritative time source when the time difference is greater than one second
(Automated)**

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must synchronize internal information system clocks to the authoritative time source when the time difference is greater than one second.

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.

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 setting time periods for different types of systems (e.g., financial, legal, or mission-critical systems).

Organizations should also consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints). This requirement is related to the comparison done every 24 hours in SRG-OS-000355 because a comparison must be done in order to determine the time difference.

Audit:

Verify the operating system synchronizes internal system clocks to the authoritative time source when the time difference is greater than one second.

Check the value of "makestep" by running the following command:

```
# grep makestep /etc/chrony/chrony.conf  
makestep 1 -1
```

If the makestep option is commented out or is not set to "1 -1", this is a finding.

Remediation:

Configure chrony to synchronize the internal system clocks to the authoritative source when the time difference is greater than one second by doing the following:

Edit the "/etc/chrony/chrony.conf" file and add:

```
makestep 1 -1
```

Restart the chrony service:

```
# systemctl restart chrony.service
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238357

Rule ID: SV-238357r654246_rule

STIG ID: UBTU-20-010436

Severity: CAT III

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.		●	●

2.1.2 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:

Verify X Windows System is not installed:

```
dpkg -l xserver-xorg*
```

Remediation:

Remove the X Windows System packages:

```
apt purge xserver-xorg*
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

2.1.3 Ensure Avahi Server is not installed (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 remove this package to reduce the potential attack surface.

Audit:

Run the following command to verify `avahi-daemon` is not installed:

```
# dpkg -s avahi-daemon | grep -E '(Status:|not installed)'  
dpkg-query: package 'avahi-daemon' is not installed and no information is  
available
```

Remediation:

Run the following commands to remove `avahi-daemon`:

```
# systemctl stop avahi-daaemon.service  
# systemctl stop avahi-daemon.socket  
# apt purge avahi-daemon
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.1.4 Ensure CUPS is not installed (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 removed to reduce the potential attack surface.

Impact:

Removing CUPS will prevent printing from the system, a common task for workstation systems.

Audit:

Run the following command to verify `cups` is not Installed:

```
# dpkg -s cups | grep -E '(Status:|not installed)'  
dpkg-query: package 'cups' is not installed and no information is available
```

Remediation:

Run one of the following commands to remove `cups` :

```
# apt purge cups
```

References:

1. More detailed documentation on CUPS is available at the project homepage at <http://www.cups.org>.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.1.5 Ensure DHCP Server is not installed (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 package be removed to reduce the potential attack surface.

Audit:

Run the following commands to verify `isc-dhcp-server` is not installed:

```
# dpkg -s isc-dhcp-server | grep -E '(Status:|not installed)'  
dpkg-query: package 'isc-dhcp-server' is not installed and no information is  
available
```

Remediation:

Run the following command to remove `isc-dhcp-server`:

```
# apt purge isc-dhcp-server
```

References:

1. More detailed documentation on DHCP is available at <http://www.isc.org/software/dhcp>.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.1.6 Ensure LDAP server 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 server, it is recommended that the software be removed to reduce the potential attack surface.

Audit:

Run the following command to verify `slapd` is not installed:

```
# dpkg -s slapd | grep -E '(Status:|not installed)'  
dpkg-query: package 'slapd' is not installed and no information is available
```

Remediation:

Run one of the following commands to remove `slapd`:

```
# apt purge slapd
```

References:

1. For more detailed documentation on OpenLDAP, go to the project homepage at <http://www.openldap.org>.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.1.7 Ensure NFS is not installed (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 or act as an NFS client, it is recommended that these services be removed to reduce the remote attack surface.

Audit:

Run the following command to verify nfs is not installed:

```
# dpkg -s nfs-kernel-server | grep -E '(Status:|not installed)'  
dpkg-query: package 'nfs-kernel-server' is not installed and no information  
is available
```

Remediation:

Run the following command to remove nfs:

```
# apt purge nfs-kernel-server
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.1.8 Ensure DNS Server is not installed (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 DNS server is not installed:

```
# dpkg -s bind9 | grep -E '(Status:|not installed)'  
dpkg-query: package 'bind9' is not installed and no information is available
```

Remediation:

Run the following commands to disable DNS server:

```
# apt purge bind9
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.1.9 Ensure FTP Server is not installed (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 installed:

```
# dpkg -s vsftpd | grep -E '(Status:|not installed)'  
dpkg-query: package 'vsftpd' is not installed and no information is available
```

Remediation:

Run the following command to remove `vsftpd`:

```
# apt purge vsftpd
```

Additional Information:

Additional FTP servers also exist and should be audited.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.1.10 Ensure HTTP server is not installed (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 `apache` is not installed:

```
# dpkg -s apache2 | grep -E '(Status:|not installed)'  
dpkg-query: package 'apache2' is not installed and no information is  
available
```

Remediation:

Run the following command to remove `apache`:

```
# apt purge apache2
```

Additional Information:

Several httpd servers exist and can use other service names. `apache2` 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 <u>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	9.2 <u>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.	●	●	●

2.1.11 Ensure IMAP and POP3 server are not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`dovecot-imapd` and `dovecot-pop3d` are 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 package be removed to reduce the potential attack surface.

Audit:

Run the following command to verify `dovecot-imapd` and `dovecot-pop3d` are not installed:

```
# dpkg -s dovecot-imapd dovecot-pop3d | grep -E '(Status:|not installed)'  
dpkg-query: package 'dovecot-imapd' is not installed and no information is available  
dpkg-query: package 'dovecot-pop3d' is not installed and no information is available
```

Remediation:

Run one of the following commands to remove `dovecot-imapd` and `dovecot-pop3d`:

```
# apt purge dovecot-imapd dovecot-pop3d
```

Additional Information:

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 <u>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	9.2 <u>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.	●	●	●

2.1.12 Ensure Samba is not installed (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 should be deleted to reduce the potential attack surface.

Audit:

Run the following command to verify `samba` is not installed:

```
# dpkg -s samba | grep -E '(Status:|not installed)'  
dpkg-query: package 'samba' is not installed and no information is available
```

Remediation:

Run the following command to remove `samba`:

```
# apt purge samba
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.1.13 Ensure HTTP Proxy Server is not installed (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 installed:

```
# dpkg -s squid | grep -E '(Status:|not installed)'  
dpkg-query: package 'squid' is not installed and no information is available
```

Remediation:

Run the following command to remove `squid`:

```
# apt purge squid
```

Additional Information:

Several HTTP proxy servers exist. These and other services should be checked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.1.14 Ensure SNMP Server is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment, computer equipment and devices like UPSs.

Net-SNMP is a suite of applications used to implement SNMPv1 (RFC 1157), SNMPv2 (RFCs 1901-1908), and SNMPv3 (RFCs 3411-3418) using both IPv4 and IPv6.

Support for SNMPv2 classic (a.k.a. "SNMPv2 historic" - RFCs 1441-1452) was dropped with the 4.0 release of the UCD-snmp package.

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 `SNMPv1`, which transmits data in the clear and does not require authentication to execute commands. `SNMPv3` replaces the simple/clear text password sharing used in `SNMPv2` with more securely encoded parameters. If the the SNMP service is not required, the `net-snmp` package should be removed to reduce the attack surface of the system.

Note: If SNMP is required:

- *The server should be configured for `SNMP v3 only`. User Authentication and Message Encryption should be configured.*
- *If `SNMP v2` is **absolutely** necessary, modify the community strings' values.*

Audit:

Run the following command to verify `snmpd` is not installed:

```
# dpkg -s snmpd | grep -E '(Status:|not installed)'  
dpkg-query: package 'snmpd' is not installed and no information is available
```

Remediation:

Run the following command to remove `snmpd`:

```
# apt purge snmpd
```

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.		●	●

2.1.15 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.

Note: This recommendation is designed around the exim4 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.

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/exim4/update-exim4.conf.conf and and or modify following lines to look like the lines below:

```
dc_eximconfig_configtype='local'  
dc_local_interfaces='127.0.0.1 ; ::1'  
dc_readhost=''  
dc_relay_domains=''  
dc_minimaldns='false'  
dc_relay_nets=''  
dc_smarthost=''  
dc_use_split_config='false'  
dc_hide_mailname=''  
dc_mailname_in_oh='true'  
dc_localdelivery='mail_spool'
```

Restart exim4:

```
# systemctl restart exim4
```

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.		●	●

2.1.16 Ensure rsync service is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsync` service can be used to synchronize files between systems over network links.

Rationale:

The `rsync` service presents a security risk as it uses unencrypted protocols for communication. The `rsync` package should be removed to reduce the attack area of the system.

Audit:

Run the following command to verify `rsync` is not installed:

```
# dpkg -s rsync | grep -E '(Status:|not installed)'  
dpkg-query: package 'rsync' is not installed and no information is available
```

Remediation:

Run the following command to remove `rsync`:

```
# apt purge rsync
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.1.17 Ensure NIS Server is not installed (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 removed and other, more secure services be used

Audit:

Run the following command to verify `nis` is not installed:

```
# dpkg -s nis | grep -E '(Status:|not installed)'  
dpkg-query: package 'nis' is not installed and no information is available
```

Remediation:

Run the following command to remove `nis`:

```
# apt purge nis
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.1.18 Ensure telnetd is not installed (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must not have the telnet package installed.

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.

Audit:

Verify that the telnet package is not installed on the Ubuntu operating system by running the following command:

```
# dpkg -l | grep telnetd
```

If the package is installed, this is a finding.

Remediation:

Remove the telnet package from the Ubuntu operating system by running the following command:

```
# apt-get remove telnetd
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238326
Rule ID: SV-238326r654153_rule
STIG ID: UBTU-20-010405
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.1.19 Ensure rsh-server is not installed (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

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).

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.

Audit:

Verify the rsh-server package is installed with the following command:

```
# dpkg -l | grep rsh-server
```

If the rsh-server package is installed, this is a finding.

Remediation:

Configure the Ubuntu operating system to disable non-essential capabilities by removing the rsh-server package from the system with the following command:

```
# apt-get remove rsh-server
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238327
Rule ID: SV-238327r654156_rule
STIG ID: UBTU-20-010406
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.		●	●

2.1.20 Ensure Endpoint Security for Linux Threat Prevention is installed (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must deploy Endpoint Security for Linux Threat Prevention (ENSLTP).

Rationale:

Without the use of automated mechanisms to scan for security flaws on a continuous and/or periodic basis, the operating system or other system components may remain vulnerable to the exploits presented by undetected software flaws.

To support this requirement, the operating system may have an integrated solution incorporating continuous scanning using HBSS and periodic scanning using other tools, as specified in the requirement.

Audit:

The Ubuntu operating system is not compliant with this requirement; hence, it is a finding. However, the severity level can be mitigated to a CAT III if the ENSLTP module is installed and running.

Check that the "mfftp" package has been installed:

```
# dpkg -l | grep mfftp
```

If the "mfftp" package is not installed, this finding will remain as a CAT II.

Check that the daemon is running:

```
# /opt/McAfee/ens/tp/init/mfetpd-control.sh status
```

If the daemon is not running, this finding will remain as a CAT II.

Remediation:

The Ubuntu operating system is not compliant with this requirement; however, the severity level can be mitigated to a CAT III if the ENSLTP module is installed and running.
Configure the Ubuntu operating system to use ENSLTP.

Install the "mfetp" package:

```
# apt-get install mfetp
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238336
Rule ID: SV-238336r654183_rule
STIG ID: UBTU-20-010415
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

2.2 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.

2.2.1 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 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 nis is not installed. Use the following command to provide the needed information:

```
# dpkg -s nis | grep -E '(Status:|not installed)'  
dpkg-query: package 'nis' is not installed and no information is available
```

Remediation:

Uninstall nis:

```
# apt purge nis
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

2.2.2 Ensure rsh client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsh-client` package contains the client commands for the `rsh` services.

Rationale:

These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the `rsh` package removes the clients for `rsh`, `rcp` and `rlogin`.

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 `rsh-client` is not installed. Use the following command to provide the needed information:

```
# dpkg -s rsh-client | grep -E '(Status:|not installed)'  
dpkg-query: package 'rsh-client' is not installed and no information is  
available
```

Remediation:

Uninstall `rsh`:

```
# apt purge rsh-client
```

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.	●	●	●

2.2.3 Ensure talk client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `talk` software makes it possible for users to send and receive messages across systems through a terminal session. The `talk` client, which allows initialization of talk sessions, is installed by default.

Rationale:

The software presents a security risk as it uses unencrypted protocols for communication.

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 `talk` is not installed. The following command may provide the needed information:

```
# dpkg -s talk | grep -E '(Status:|not installed)'  
dpkg-query: package 'talk' is not installed and no information is available
```

Remediation:

Uninstall `talk`:

```
# apt purge talk
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

2.2.4 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. Use the following command to provide the needed information:

```
# dpkg -s telnet | grep -E '(Status:|not installed)'  
dpkg-query: package 'telnet' is not installed and no information is available
```

Remediation:

Uninstall `telnet`:

```
# apt purge 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.	●	●	●

2.2.5 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 that `ldap-utils` is not installed. Use the following command to provide the needed information:

```
# dpkg -s ldap-utils | grep -E '(Status:|not installed)'  
dpkg-query: package 'ldap-utils' is not installed and no information is  
available
```

Remediation:

Uninstall `ldap-utils`:

```
# apt purge ldap-utils
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

2.2.6 Ensure RPC is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Remote Procedure Call (RPC) is a method for creating low level client server applications across different system architectures. It requires an RPC compliant client listening on a network port. The supporting package is rpcbind."

Rationale:

If RPC is not required, it is recommended that this services be removed to reduce the remote attack surface.

Audit:

Run the following command to verify `rpcbind` is not installed:

```
# dpkg -s rpcbind | grep -E '(Status:|not installed)'  
dpkg-query: package 'rpcbind' is not installed and no information is  
available
```

Remediation:

Run the following command to remove `rpcbind`:

```
# apt purge rpcbind
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

2.3 Ensure nonessential services are removed or masked (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A network port is identified by its number, the associated IP address, and the type of the communication protocol such as TCP or UDP.

A listening port is a network port on which an application or process listens on, acting as a communication endpoint.

Each listening port can be open or closed (filtered) using a firewall. In general terms, an open port is a network port that accepts incoming packets from remote locations.

Rationale:

Services listening on the system pose a potential risk as an attack vector. These services should be reviewed, and if not required, the service should be stopped, and the package containing the service should be removed. If required packages have a dependency, the service should be stopped and masked to reduce the attack surface of the system.

Audit:

Run the following command:

```
# lsof -i -P -n | grep -v "(ESTABLISHED)"
```

Review the output to ensure that all services listed are required on the system. If a listed service is not required, remove the package containing the service. If the package containing a non-essential service is required, stop and mask the non-essential service.

Remediation:

Run the following command to remove the package containing the service:

```
# apt purge <package_name>
```

OR If required packages have a dependency:

Run the following command to stop and mask the service:

```
# systemctl --now mask <service_name>
```

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 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 Disable unused network protocols and devices

To reduce the attack surface of a system, unused network protocols and devices should be disabled.

3.1.1 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.

Impact:

If IPv6 is disabled through sysctl config, `SSH X11forwarding` may no longer function as expected. We recommend that SSH X11forwarding be disabled, but if required, the following will allow for `SSH X11forwarding` with IPv6 disabled through sysctl config:

Add the following line the `/etc/ssh/sshd_config` file:

```
AddressFamily inet
```

Run the following command to re-start the openSSH server:

```
# systemctl restart sshd
```

Audit:

Run one of the following commands to verify IPv6 is disabled:

IF IPv6 is disabled through grub

Run the following command:

```
# grep "^\s*linux" /boot/grub/grub.cfg | grep -v "ipv6.disable=1"
```

no lines should be returned

OR

IF IPv6 is disabled through sysctl settings:

Run the following commands:

```
# sysctl net.ipv6.conf.all.disable_ipv6  
  
net.ipv6.conf.all.disable_ipv6 = 1  
  
# sysctl net.ipv6.conf.default.disable_ipv6  
  
net.ipv6.conf.default.disable_ipv6 = 1  
  
# grep -E  
'^\s*net\.ipv6\.conf\.(all|default)\.disable_ipv6\s*=\s*\b(\s+\#\.*\)?\$'  
/etc/sysctl.conf /etc/sysctl.d/*.*.conf | cut -d: -f2  
  
net.ipv6.conf.all.disable_ipv6 = 1  
net.ipv6.conf.default.disable_ipv6 = 1
```

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:

```
# update-grub
```

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	9.4 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.	●	●	●

3.1.2 Ensure wireless interfaces are disabled (Automated)

Profile Applicability:

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

Description:

Wireless networking is used when wired networks are unavailable. Debian 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 script to verify no wireless interfaces are active on the system:

```
#!/bin/bash

if command -v nmcli >/dev/null 2>&1 ; then
    if nmcli radio all | grep -Eq '\s*\S+\s+disabled\s+\S+\s+disabled\b'; then
        echo "Wireless is not enabled"
    else
        nmcli radio all
    fi
elif [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
    t=0
    mname=$(for driverdir in $(find /sys/class/net/*/ -type d -name wireless | xargs -0 dirname); do basename "$(readlink -f "$driverdir"/device/driver/module)"; done | sort -u)
    for dm in $mname; do
        if grep -Eq "^\s*install\s+$dm\s+/bin/(true|false)" /etc/modprobe.d/*.conf; then
            /bin/true
        else
            echo "$dm is not disabled"
            t=1
        fi
    done
    [ "$t" -eq 0 ] && echo "Wireless is not enabled"
else
    echo "Wireless is not enabled"
fi
```

Output should be:

```
Wireless is not enabled
```

Remediation:

Run the following script to disable any wireless interfaces:

```
#!/bin/bash

if command -v nmcli >/dev/null 2>&1 ; then
    nmcli radio all off
else
    if [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
        mname=$(for driverdir in $(find /sys/class/net/*/ -type d -name wireless | xargs -0 dirname); do basename "$(readlink -f "$driverdir"/device/driver/module)"; done | sort -u)
        for dm in $mname; do
            echo "install $dm /bin/true" >> /etc/modprobe.d/disable_wireless.conf
        done
    fi
fi
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238375
Rule ID: SV-238375r654300_rule
STIG ID: UBTU-20-010455
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.			●

3.2 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:

Configuration files are read from directories in `/etc/`, `/run/`, `/usr/local/lib/`, and `/lib/`, in order of precedence. Files must have the ".conf" extension. Files in `/etc/` override files with the same name in `/run/`, `/usr/local/lib/`, and `/lib/`. Files in `/run/` override files with the same name under `/usr/`.

All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Thus, the configuration in a certain file may either be replaced completely (by placing a file with the same name in a directory with higher priority), or individual settings might be changed (by specifying additional settings in a file with a different name that is ordered later).

Packages should install their configuration files in `/usr/lib/` (distribution packages) or `/usr/local/lib/` (local installs). Files in `/etc/` are reserved for the local administrator, who may use this logic to override the configuration files installed by vendor packages. It is recommended to prefix all filenames with a two-digit number and a dash, to simplify the ordering of the files.

If the administrator wants to disable a configuration file supplied by the vendor, the recommended way is to place a symlink to `/dev/null` in the configuration directory in `/etc/`, with the same filename as the vendor configuration file. If the vendor configuration file is included in the initrd image, the image has to be regenerated.

3.2.1 Ensure packet redirect sending is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 -E "\s*net\.ipv4\.conf\.all\.send_redirects" /etc/sysctl.conf  
/etc/sysctl.d/*  
  
net.ipv4.conf.all.send_redirects = 0  
  
# grep -E "\s*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
```

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 IP forwarding is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```

#!/usr/bin/bash

output=""
grubfile=$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="IPv6 disabled in grub config"
grep -Eqs "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eqs
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="IPv6 disabled in sysctl config"
[ -n "$output" ] && echo -e "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"

```

Remediation:

Run the following command to restore the default parameter and set the active kernel parameter:

```

# 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*\S+\b)\s*$/#
*REMOVED* \1/" $filename; done; sysctl -w net.ipv4.ip_forward=0; sysctl -w
net.ipv4.route.flush=1

```

IF IPv6 is enabled:

Run the following command to restore the default parameter and set the active kernel parameter:

```

# 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*\S+\b)\s*$/#
*REMOVED* \1/" $filename; done; sysctl -w net.ipv6.conf.all.forwarding=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.	●	●	●

3.3 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:

Configuration files are read from directories in `/etc/`, `/run/`, `/usr/local/lib/`, and `/lib/`, in order of precedence. Files must have the ".conf" extension. Files in `/etc/` override files with the same name in `/run/`, `/usr/local/lib/`, and `/lib/`. Files in `/run/` override files with the same name under `/usr/`.

All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Thus, the configuration in a certain file may either be replaced completely (by placing a file with the same name in a directory with higher priority), or individual settings might be changed (by specifying additional settings in a file with a different name that is ordered later).

Packages should install their configuration files in `/usr/lib/` (distribution packages) or `/usr/local/lib/` (local installs). Files in `/etc/` are reserved for the local administrator, who may use this logic to override the configuration files installed by vendor packages. It is recommended to prefix all filenames with a two-digit number and a dash, to simplify the ordering of the files.

If the administrator wants to disable a configuration file supplied by the vendor, the recommended way is to place a symlink to `/dev/null` in the configuration directory in `/etc/`, with the same filename as the vendor configuration file. If the vendor configuration file is included in the initrd image, the image has to be regenerated.

3.3.1 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/*  
  
net.ipv4.conf.all.accept_source_route= 0  
  
# grep "net\.ipv4\.conf\.default\.accept_source_route" /etc/sysctl.conf  
/etc/sysctl.d/*  
  
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/*  
  
net.ipv6.conf.all.accept_source_route= 0  
  
# grep "net\.ipv6\.conf\.default\.accept_source_route" /etc/sysctl.conf  
/etc/sysctl.d/*  
  
net.ipv6.conf.default.accept_source_route= 0
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```

#!/usr/bin/bash

output=""
grubfile=$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eq "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eq
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"

```

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 enabled:

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.	●	●	●

3.3.2 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/*  
  
net.ipv4.conf.all.accept_redirects= 0  
  
# grep "net\.ipv4\conf\default\accept_redirects" /etc/sysctl.conf  
/etc/sysctl.d/*  
  
net.ipv4.conf.default.accept_redirects= 0
```

IF IPv6 is enabled:

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/*
net.ipv6.conf.all.accept_redirects= 0

# grep "net\.ipv6\conf\default\accept_redirects" /etc/sysctl.conf
/etc/sysctl.d/*
net.ipv6.conf.default.accept_redirects= 0

```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```

#!/usr/bin/bash

output=""
grubfile=$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eq "^\s*net\.ipv6\conf\all\disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eq
"^\s*net\.ipv6\conf\default\disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\conf\all\disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\conf\default\disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"

```

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 enabled:

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.	●	●	●

3.3.3 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.	●	●	●

3.3.4 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	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	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.		●	●

3.3.5 Ensure broadcast ICMP requests are ignored (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 "net\.ipv4\.icmp_echo_ignore_broadcasts" /etc/sysctl.conf  
/etc/sysctl.d/*  
  
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=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.	●	●	●

3.3.6 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 "net.ipv4.icmp_ignore_bogus_error_responses" /etc/sysctl.conf  
/etc/sysctl.d/*  
  
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=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.	●	●	●

3.3.7 Ensure Reverse Path Filtering is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 "net\.ipv4\.conf\.all\.rp_filter" /etc/sysctl.conf /etc/sysctl.d/*
net.ipv4.conf.all.rp_filter = 1

# grep "net\.ipv4\.conf\.default\.rp_filter" /etc/sysctl.conf /etc/sysctl.d/*
net.ipv4.conf.default.rp_filter = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.all.rp_filter = 1  
net.ipv4.conf.default.rp_filter = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.rp_filter=1  
  
# sysctl -w net.ipv4.conf.default.rp_filter=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.	●	●	●

3.3.8 Ensure TCP SYN Cookies is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG - Server
- STIG - 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 "net\.ipv4\.tcp_syncookies" /etc/sysctl.conf /etc/sysctl.d/*  
net.ipv4.tcp_syncookies = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.tcp_syncookies = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.tcp_syncookies=1  
# sysctl -w net.ipv4.route.flush=1
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238333
Rule ID: SV-238333r654174_rule
STIG ID: UBTU-20-010412
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.	●	●	●

3.3.9 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
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```

#!/usr/bin/bash

output=""
grubfile=$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="IPv6 disabled in grub config"
grep -Eq "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eq
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="IPv6 disabled in sysctl config"
[ -n "$output" ] && echo -e "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"

```

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	<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>	●	●	●

3.4 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.

3.4.1 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: `vi /etc/modprobe.d/dccp.conf`

Add the following line:

```
install dccp /bin/true
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

3.4.2 Ensure SCTP is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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 | grep -E '(sctp|install)'  
install /bin/true  
  
# lsmod | grep sctp  
  
<No output>
```

Remediation:

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

Example: vi /etc/modprobe.d/sctp.conf
and add the following line:

```
install sctp /bin/true
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

3.4.3 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: vi /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	4.8 <u>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	9.2 <u>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.	●	●	●

3.4.4 Ensure TIPC is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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 | grep -E '(tipc|install)'  
install /bin/true  
  
# lsmod | grep tipc  
  
<No output>
```

Remediation:

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

Example: `vi /etc/modprobe.d/tipc.conf`

and add the following line:

```
install tipc /bin/true
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>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.	●	●	●

3.5 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:

- UncomplicatedFirewall (ufw) - Provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the iptables backend. ufw supports both IPv4 and IPv6 networks
- 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.

Notes:

- *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*

3.5.1 Configure Uncomplicated Firewall

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.

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed to be easy to use.

- Uses a command-line interface consisting of a small number of simple commands
- Uses iptables for configuration
- Rules are processed until first matching rule. The first matching rule will be applied.

Notes:

- *Configuration of a live system's firewall directly over a remote connection will often result in being locked out*
- *Rules should be ordered so that ALLOW rules come before DENY rules.*

3.5.1.1 Ensure ufw is installed (Automated)

Profile Applicability:

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

Description:

The Uncomplicated Firewall (ufw) is a frontend for iptables and is particularly well-suited for host-based firewalls. ufw provides a framework for managing netfilter, as well as a command-line interface for manipulating the firewall

Rationale:

A firewall utility is required to configure the Linux kernel's netfilter framework via the iptables or nftables back-end.

The Linux kernel's netfilter framework host-based firewall can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

Note: Only one firewall utility should be installed and configured. UFW is dependent on the iptables package

Audit:

Run the following command to verify that Uncomplicated Firewall (UFW) is installed:

```
# dpkg -s ufw | grep 'Status: install'  
Status: install ok installed
```

Remediation:

Run the following command to install Uncomplicated Firewall (UFW):

```
apt install ufw
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238354
Rule ID: SV-238354r654237_rule
STIG ID: UBTU-20-010433
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.	●	●	●

3.5.1.2 Ensure `iptables-persistent` is not installed with `ufw` (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `iptables-persistent` is a boot-time loader for netfilter rules, `iptables` plugin

Rationale:

Running both `ufw` and the services included in the `iptables-persistent` package may lead to conflict

Audit:

Run the following command to verify that the `iptables-persistent` package is not installed:

```
dpkg-query -s iptables-persistent  
package 'iptables-persistent' is not installed and no information is available
```

Remediation:

Run the following command to remove the `iptables-persistent` package:

```
# apt purge iptables-persistent
```

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.	●	●	●

3.5.1.3 Ensure ufw service is enabled (Automated)

Profile Applicability:

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

Description:

UncomplicatedFirewall (ufw) is a frontend for iptables. ufw provides a framework for managing netfilter, as well as a command-line and available graphical user interface for manipulating the firewall.

Notes:

- When running `ufw enable` or starting ufw via its initscript, ufw will flush its chains. This is required so ufw can maintain a consistent state, but it may drop existing connections (eg ssh). ufw does support adding rules before enabling the firewall.
- Run the following command before running `ufw enable`.

```
# ufw allow proto tcp from any to any port 22
```

- The rules will still be flushed, but the ssh port will be open after enabling the firewall. Please note that once ufw is 'enabled', ufw will not flush the chains when adding or removing rules (but will when modifying a rule or changing the default policy)
- By default, ufw will prompt when enabling the firewall while running under ssh. This can be disabled by using `ufw --force enable`

Rationale:

The ufw service must be enabled and running in order for ufw to protect the system

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 ufw is enabled:

```
# systemctl is-enabled ufw  
enabled
```

Run the following command to verify that ufw is running:

```
# ufw status | grep Status  
Status: active
```

Remediation:

Run the following command to enable ufw:

```
# ufw enable
```

References:

1. <http://manpages.ubuntu.com/manpages/precise/en/man8/ufw.8.html>

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238355
Rule ID: SV-238355r654240_rule
STIG ID: UBTU-20-010434
Severity: CAT II

Vul ID: V-238374
Rule ID: SV-238374r654297_rule
STIG ID: UBTU-20-010454
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.	●	●	●

3.5.1.4 Ensure ufw 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 for IPv4 and ::1/128 for IPv6).

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 for IPv4 and ::1/128 for IPv6) 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:

```
# ufw status verbose

To                      Action      From
--                      ----      ---
Anywhere on lo          ALLOW IN   Anywhere
Anywhere                DENY IN    127.0.0.0/8
Anywhere (v6) on lo     ALLOW IN   Anywhere (v6)
Anywhere (v6)            DENY IN   ::1

Anywhere                  ALLOW OUT  Anywhere on lo
Anywhere (v6)             ALLOW OUT  Anywhere (v6) on lo
```

Remediation:

Run the following commands to implement the loopback rules:

```
# ufw allow in on lo
# ufw allow out on lo
# ufw deny in from 127.0.0.0/8
# ufw deny in from ::1
```

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.	●	●	●

3.5.1.5 Ensure ufw outbound connections are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound connections.

Notes:

- *Changing firewall settings while connected over network can result in being locked out of the system.*
- *Unlike iptables, when a new outbound rule is added, ufw automatically takes care of associated established connections, so no rules for the latter kind are required.*

Rationale:

If rules are not in place for new outbound 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 connections match site policy:

```
# ufw status numbered
```

Remediation:

Configure ufw in accordance with site policy. The following commands will implement a policy to allow all outbound connections on all interfaces:

```
# ufw allow out on all
```

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.	●	●	●

3.5.1.6 Ensure ufw firewall rules exist for all open ports (Manual)

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.

Notes:

- *Changing firewall settings while connected over network can result in being locked out of the system*
- *The remediation command opens up the port to traffic from all sources. Consult ufw documentation and set any restrictions in compliance with site policy*

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 Local Address:Port	State	Recv-Q	Peer Address:Port	Send-Q
udp 127.0.0.53%lo:53	UNCONN	0	0.0.0.0:*	0
udp 10.105.106.117%enp1s0:68	UNCONN	0	0.0.0.0:*	0
tcp 127.0.0.53%lo:53	LISTEN	0	0.0.0.0:*	128
tcp 0.0.0.0:22	LISTEN	0	0.0.0.0:*	128

Run the following command to determine firewall rules:

```
# ufw status verbose
```

Status: active		
To	Action	From
--	-----	----
[1] Anywhere on lo	ALLOW IN	Anywhere
[2] Anywhere	ALLOW OUT	Anywhere on lo (out)
[3] Anywhere	DENY IN	127.0.0.0/8
[4] 22/tcp	ALLOW IN	Anywhere
[5] Anywhere	ALLOW OUT	Anywhere on enp1s0 (out)
[6] Anywhere	ALLOW OUT	Anywhere on all (out)
[7] Anywhere (v6) on lo	ALLOW IN	Anywhere (v6)
[8] Anywhere (v6)	ALLOW OUT	Anywhere (v6) on lo (out)
[9] Anywhere (v6)	DENY IN	::1
[10] 22/tcp (v6)	ALLOW IN	Anywhere (v6)
[11] Anywhere (v6)	ALLOW OUT	Anywhere (v6) on all (out)

Verify all open ports listening on non-localhost addresses have at least one firewall rule.
Lines identified by indexes 4 and 10 are firewall rules 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:

```
# ufw allow in <port>/<tcp or udp protocol>
```

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.	●	●	●

3.5.1.7 Ensure ufw default deny firewall policy (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A default deny policy on connections ensures that any unconfigured network usage will be rejected.

Note: Any port or protocol without a explicit allow before the default deny will be blocked

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.

Impact:

Any port and protocol not explicitly allowed will be blocked. The following rules should be considered before applying the default deny.

```
ufw allow git  
ufw allow in http  
ufw allow in https  
ufw allow out 53  
  
ufw logging on
```

Audit:

Run the following command and verify that the default policy for **incoming**, **outgoing**, and **routed** directions is **deny** or **reject**:

```
# ufw status verbose
```

Remediation:

Run the following commands to implement a default *deny* policy:

```
# ufw default deny incoming  
# ufw default deny outgoing  
# ufw default deny routed
```

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.	●	●	●

3.5.1.8 Ensure functions, ports, protocols, and services are restricted (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the PPSM CAL and vulnerability assessments.

Rationale:

In order 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:

Verify the Ubuntu operating system is 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. Check the firewall configuration for any unnecessary or prohibited functions, ports, protocols, and/or services by running the following command:

```
# ufw show raw

Chain OUTPUT (policy ACCEPT)
target prot opt sources destination
Chain INPUT (policy ACCEPT 1 packets, 40 bytes)
pkts bytes target prot opt in out source destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
```

Ask the System Administrator

for the site or program PPSM CLSA. Verify the services allowed by the firewall match the PPSM CLSA.

If there are any additional ports, protocols, or services that are not included in the PPSM CLSA, this is a finding.

If there are any ports, protocols, or services that are prohibited by the PPSM CAL, this is a finding.

Remediation:

Add all ports, protocols, or services allowed by the PPSM CLSA by using the following command:

```
# ufw allow <direction> <port/protocol/service>
```

where the direction is "in" or "out" and the port is the one corresponding to the protocol or service allowed.

To deny access to ports, protocols, or services, use:

```
# ufw deny <direction> <port/protocol/service>
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238328
Rule ID: SV-238328r654159_rule
STIG ID: UBTU-20-010407
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.	●	●	●
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

3.5.1.9 Ensure UFW rate-limits impacted network interfaces (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must configure the uncomplicated firewall to rate-limit impacted network interfaces.

Rationale:

Denial of service (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 exist 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.

Audit:

Verify an application firewall is configured to rate limit any connection to the system. Check all the services listening to the ports with the following command:

```
# ss -l46ut  
  
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process  
tcp LISTEN 0 128 [::]:ssh [::]:*
```

For each entry, verify that the Uncomplicated Firewall is configured to rate limit the service ports with the following command:

```
# ufw status  
  
Status: active  
  
To Action From  
-- -----  
22/tcp LIMIT Anywhere  
22/tcp (v6) LIMIT Anywhere (v6)
```

If any port with a state of "LISTEN" is not marked with the "LIMIT" action, this is a finding.

Remediation:

Configure the application firewall to protect against or limit the effects of DoS attacks by ensuring the Ubuntu operating system is implementing rate-limiting measures on impacted network interfaces.

Check all the services listening to the ports with the following command:

```
# ss -l46ut  
  
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process  
tcp LISTEN 0 128 [::]:ssh [::]:*
```

For each service with a port listening to connections, run the following command, replacing "[service]" with the service that needs to be rate limited.

```
# ufw limit [service]
```

Rate-limiting can also be done on an interface. An example of adding a rate-limit on the eth0 interface follows:

```
# ufw limit in on eth0
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238367
Rule ID: SV-238367r654276_rule
STIG ID: UBTU-20-010446
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.	●	●	●
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

3.5.2 Configure nftables

If Uncomplicated Firewall (UFW) 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. Please ensure that your kernel supports nf_tables before choosing this option.

Notes:

- *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.*

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.rules

```

#!/sbin/nft -f

# This nftables.rules config should be saved as /etc/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.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.rules
```

Add the following line to /etc/nftables.conf

```
include "/etc/nftables.rules"
```

3.5.2.1 Ensure nftables is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM) and a new nft userspace command line tool. nftables reuses the existing Netfilter subsystems such as the existing hook infrastructure, the connection tracking system, NAT, userspace queuing and logging subsystem.

Notes:

- *nftables is available in Linux kernel 3.13 and newer*
- *Only one firewall utility should be installed and configured*
- *Changing firewall settings while connected over the network can result in being locked out of the system*

Rationale:

nftables is a subsystem of the Linux kernel that can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

Audit:

Run the following command to verify that nftables is installed:

```
# dpkg-query -s nftables | grep 'Status: install ok installed'  
Status: install ok installed
```

Remediation:

Run the following command to install nftables:

```
# apt install 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.	●	●	●

3.5.2.2 Ensure ufw is uninstalled or disabled with nftables (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed to be easy to use.

Rationale:

Running both the nftables service and ufw may lead to conflict and unexpected results.

Audit:

Run the following commands to verify that ufw is *either* not installed or inactive. *Only one of the following needs to pass.*

Run the following command to verify that ufw is not installed:

```
# dpkg-query -s ufw | grep 'Status: install ok installed'  
package 'ufw' is not installed and no information is available
```

Run the following command to verify ufw is disabled:

```
# ufw status  
Status: inactive
```

Remediation:

Run *one* of the following commands to either remove ufw or disable ufw

Run the following command to remove ufw:

```
# apt purge ufw
```

Run the following command to disable ufw:

```
# ufw disable
```

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.	●	●	●

3.5.2.3 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	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.	●	●	●

3.5.2.4 Ensure a 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.	●	●	●

3.5.2.5 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.

```
# nft list ruleset | grep 'hook input'  
type filter hook input priority 0;
```

Run the following commands and verify that base chains exist for FORWARD.

```
# nft list ruleset | grep 'hook forward'  
type filter hook forward priority 0;
```

Run the following commands and verify that base chains exist for OUTPUT.

```
# 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.	●	●	●

3.5.2.6 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 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 on the system:

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 on the system:

Run the following command to implement the IPv6 loopback rule:

```
# nft add rule inet filter input ip6 saddr ::1 counter drop
```

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.	●	●	●

3.5.2.7 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.	●	●	●

3.5.2.8 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.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

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

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.	●	●	●

3.5.2.9 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 on the nftables service

Rationale:

The nftables service restores the nftables rules from the rules files referenced in the /etc/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 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.	●	●	●

3.5.2.10 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/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:

Run the following command to verify the input base chain:

```
# [ -n "$(grep -E '^\\s*include' /etc/nftables.conf)" ] && awk '/hook  
input/,/}/' $(awk '$1 ~ /^\\s*include/ { gsub("\\\"", "", $2); print $2 }'  
/etc/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
```

Review the input base chain to ensure that it follows local site policy

Run the following command to verify the forward base chain:

```
# [ -n "$(grep -E '^\\s*include' /etc/nftables.conf)" ] && awk '/hook  
forward/,/}/' $(awk '$1 ~ /^\\s*include/ { gsub("\\\"", "", $2); print $2 }'  
/etc/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;  
}
```

Review the forward base chain to ensure that it follows local site policy.

Run the following command to verify the forward base chain:

```
# [ -n "$(grep -E '^s*include' /etc/nftables.conf)" ] && awk '/hook output/,/}/' $(awk '$1 ~ /^s*include/ { gsub("\\"","\"",\$2);print \$2 }' /etc/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
}
```

Review the output base chain to ensure that it follows local site policy.

Remediation:

Edit the `/etc/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/nftables.conf
```

Add the line:

```
include "/etc/nftables.rules"
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.4 Implement and Manage a Firewall on Servers</p> <p>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</p> <p>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>	●	●	●

3.5.3 Configure iptables

If Uncomplicated Firewall (UFW) 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 system's firewall directly over a remote connection will often result in being locked out

3.5.3.1 Configure iptables software

This section provides guidance for installing, enabling, removing, and disabling software packages necessary for using IPTables as the method for configuring and maintaining a Host Based Firewall on the system.

Note: Using more than one method to configure and maintain a Host Based Firewall can cause unexpected results. If FirewallD or NFTables are being used for configuration and maintenance, this section should be skipped and the guidance in their respective section followed.

3.5.3.1.1 Ensure iptables packages are installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

iptables is a utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall, implemented as different Netfilter modules, and the chains and rules it stores. Different kernel modules and programs are used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.

Rationale:

A method of configuring and maintaining firewall rules is necessary to configure a Host Based Firewall.

Audit:

Run the following command to verify that `iptables` and `iptables-persistent` are installed:

```
# apt list iptables iptables-persistent | grep installed  
iptables-persistent/<version> [installed,automatic]  
iptables/<version> [installed,automatic]
```

Remediation:

Run the following command to install `iptables` and `iptables-persistent`

```
# apt install iptables iptables-persistent
```

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.	●	●	●

3.5.3.1.2 Ensure nftables is not installed with iptables (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.

Rationale:

Running both `iptables` and `nftables` may lead to conflict.

Audit:

Run the following command to verify that nftables is not installed:

```
# dpkg -s nftables  
dpkg-query: package 'nftables' is not installed
```

Remediation:

Run the following command to remove `nftables`:

```
# apt purge 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.	●	●	●

3.5.3.1.3 Ensure ufw is uninstalled or disabled with iptables (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed to be easy to use.

- Uses a command-line interface consisting of a small number of simple commands
- Uses iptables for configuration

Rationale:

Running `iptables.persistent` with ufw enabled may lead to conflict and unexpected results.

Audit:

Run the following commands to verify that `ufw` is *either* not installed or disabled. *Only one of the following needs to pass.*

Run the following command to verify that `ufw` is not installed:

```
# dpkg-query -s ufw
package 'ufw' is not installed and no information is available
```

Run the following command to verify ufw is disabled:

```
# ufw status
Status: inactive
```

Run the following commands to verify that the `ufw` service is masked:

```
# systemctl is-enabled ufw
masked
```

Remediation:

Run *one* of the following commands to either remove ufw or stop and mask ufw
Run the following command to remove ufw:

```
# apt purge ufw
```

OR

Run the following commands to disable ufw:

```
# ufw disable
```

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.	●	●	●

3.5.3.2 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). 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. The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere:

```
#!/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
```

3.5.3.2.1 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).

Notes:

- *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*

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
```

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.	●	●	●

3.5.3.2.2 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.

Notes:

- *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*

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
```

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.	●	●	●

3.5.3.2.3 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.

Notes:

- *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*

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
```

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.	●	●	●

3.5.3.2.4 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.

Note:

- 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

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	policy	pkts	bytes	target	prot	opt	in	out	source	destination
INPUT	DROP	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
```

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>9.2 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.</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>	●	●	●

3.5.3.3 Configure IPv6 ip6tables

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.

If IPv6 is enabled on the system, the ip6tables should be configured.

Note: This section broadly assumes starting with an empty ip6tables firewall ruleset (established by flushing the rules with ip6tables -F). 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.

The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere:

```
#!/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
```

3.5.3.3.1 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).

Note:

- 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

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:

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
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/bash

output=""
grubfile=$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -EqS "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -EqS
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

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
```

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.	●	●	●

3.5.3.3.2 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.

Note:

- 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

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:

```
# ip6tables -L -v -n
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/bash

output=""
grubfile=$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -EqS "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -EqS
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

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
```

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.	●	●	●

3.5.3.3.3 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.

Note:

- 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

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:

```
# ip6tables -L
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/bash

output=""
grubfile=$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eq "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eq
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# ip6tables -P INPUT DROP
# ip6tables -P OUTPUT DROP
# ip6tables -P FORWARD DROP
```

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.	●	●	●

3.5.3.3.4 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.

Note:

- 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

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 -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.

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/bash

output=""
grubfile=$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eq "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eq
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

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
```

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.	●	●	●

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.

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 AppArmor 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.

Notes:

- *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*
- *Audit rules that have `archas` a rule parameter:*
 - *On 64 bit systems, you will need two rules, one for 64 bit and one for 32 bit*
 - *On 32 bit systems, only the 32 bit rule is needed*
- *Several recommendations in this section filter based off of `auid>=1000` for unprivileged non-system users. Some systems may have a non-default `UID_MIN` setting, consult the `UID_MIN` setting in `/etc/login.defs` to determine the `UID_MIN` setting for your system*
- *The audits in this section look for a `key` value. The `key` value may be different for the audit rules on your system. If a different `key` value, denoted by `-k` or `key=` is used on your system, please replace the `grep <key_value>` with the `key` value in use on your system*
- *Once all audit rules have been added to a file or files in the `/etc/audit/rules.d/` directory, the `auditd` service must be re-started, or the system rebooted, for the new rules to be included*

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 - Server
- STIG - Workstation

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:

```
# dpkg -s auditd audispd-plugins
```

Remediation:

Run the following command to Install auditd

```
# apt install auditd audispd-plugins
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238298
Rule ID: SV-238298r654069_rule
STIG ID: UBTU-20-010182
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.	●	●	●

4.1.1.2 Ensure auditd service is enabled (Automated)

Profile Applicability:

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

Description:

Enable and start 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:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238298
Rule ID: SV-238298r654069_rule
STIG ID: UBTU-20-010182
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.	●	●	●

4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated)

Profile Applicability:

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

Description:

Configure `grub` so that processes that are capable of being audited can be audited even if they start up prior to `auditd` startup.

Note: This recommendation is designed around the `grub` bootloader, if `LILO` or another bootloader is in use in your environment enact equivalent settings. Replace `/boot/grub/grub.cfg` with the appropriate `grub` configuration file for your environment.

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 and verify that each `linux` line has the `audit=1` parameter set:

```
# grep "^\s*linux" /boot/grub/grub.cfg | grep -v "audit=1"
```

Nothing should be returned

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:

```
# update-grub
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238299
Rule ID: SV-238299r654072_rule
STIG ID: UBTU-20-010198
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.	●	●	●

4.1.1.4 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 commands and verify the `audit_backlog_limit=` parameter is set to an appropriate size for your organization

```
# grep "^\s*linux" /boot/grub/grub.cfg | grep -v "audit_backlog_limit="
```

Nothing should be returned

```
# grep "audit_backlog_limit=" /boot/grub/grub.cfg
```

Ensure the returned value complies with local site policy

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:

```
# update-grub
```

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.

Notes:

- *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*

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>
```

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
- STIG - Server
- STIG - 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
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238243
Rule ID: SV-238243r653904_rule
STIG ID: UBTU-20-010117
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.		●	●

4.1.2.4 Ensure shut down by default upon audit failure (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must shut down by default upon audit failure (unless availability is an overriding concern).

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), 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 Ubuntu 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, this is a finding.

Remediation:

Configure the Ubuntu 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", "HALT" or "SINGLE") in "/etc/audit/auditd.conf" file:

```
disk_full_action = HALT
```

Restart the "auditd" service so the changes take effect:

```
# systemctl restart auditd.service
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238244
Rule ID: SV-238244r653907_rule
STIG ID: UBTU-20-010118
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	6.4 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 sufficient storage capacity to store at least one week worth of audit records (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must allocate audit record storage capacity to store at least one weeks' worth of audit records, when audit records are not immediately sent to a central audit record storage facility.

Rationale:

In order to ensure operating systems have a sufficient storage capacity in which to write the audit logs, operating systems need to be able to allocate audit record storage capacity.

Audit:

Verify the Ubuntu operating system allocates audit record storage capacity to store at least one week's worth of audit records when audit records are not immediately sent to a central audit record storage facility.

Determine which partition the audit records are being written to with the following command:

```
# grep ^log_file /etc/audit/auditd.conf  
log_file = /var/log/audit/audit.log
```

Check the size of the partition that audit records are written to (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
```

Note: The partition size needed to capture a week's worth of audit records is based on the activity level of the system and the total storage capacity available. In normal circumstances, 10.0 GB of storage space for audit records will be sufficient.

If the audit record partition is not allocated for sufficient storage capacity, this is a finding.

Remediation:

Allocate enough storage capacity for at least one week's worth 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, use the "parted" program to resize the partition with sufficient space to contain one week's worth of audit records.

If audit records are not stored on a partition made specifically for audit records, a new partition with sufficient amount of space will need to be created.

Set the audited server to point to the mount point where the audit records must be located:

```
# sed -i -E 's@^(log_file\s*=\\s*) .*@\1 <log mountpoint>/audit.log@' /etc/audit/auditd.conf
```

Where is the aforementioned mount point.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238305
Rule ID: SV-238305r654090_rule
STIG ID: UBTU-20-010215
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.		●	●

4.1.2.6 Ensure audit event multiplexor is configured to off-load audit logs onto a different system or storage media from the system being audited (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system audit event multiplexor must be configured to off-load audit logs 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.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify the audit event multiplexor is configured to offload audit records to a different system or storage media from the system being audited.

Check that audisp-remote plugin is installed:

```
# dpkg -s audisdp-plugins
```

If status is "not installed", this is a finding.

Check that the records are being offloaded to a remote server with the following command:

```
# grep -i active /etc/audisp/plugins.d/au-remote.conf  
active = yes
```

If "active" is not set to "yes", or the line is commented out, this is a finding.

Check that audisp-remote plugin is configured to send audit logs to a different system:

```
# grep -i ^remote_server /etc/audisp/audisp-remote.conf  
remote_server = 192.168.122.126
```

If the "remote_server" parameter is not set, is set with a local address, or is set with an invalid address, this is a finding.

Remediation:

Configure the audit event multiplexor to offload audit records to a different system or storage media from the system being audited.

Install the audisp-remote plugin:

```
# apt-get install audispd-plugins -y
```

Set the audisp-remote plugin as active by editing the "/etc/audisp/plugins.d/au-remote.conf" file:

```
# sed -i -E 's/active\s*=\\s*no/active = yes/' /etc/audisp/plugins.d/au-remote.conf
```

Set the address of the remote machine by editing the "/etc/audisp/audisp-remote.conf" file:

```
# sed -i -E 's/(remote_server\s*=).*/\1 <remote addr>/' /etc/audisp/audisp-remote.conf
```

Where must be substituted by the address of the remote server receiving the audit log.

Make the audit service reload its configuration files:

```
# systemctl restart auditd.service
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238306
Rule ID: SV-238306r654093_rule
STIG ID: UBTU-20-010216
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.	●	●	●

4.1.2.7 Ensure security personnel are notified when storage volume reaches 75 percent utilization (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must immediately notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity.

Rationale:

If security personnel are not notified immediately when storage volume reaches 75% utilization, they are unable to plan for audit record storage capacity expansion.

Audit:

Verify the Ubuntu operating system notifies the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity with the following command:

```
# grep ^space_left_action /etc/audit/auditd.conf  
space_left_action email  
  
# grep ^space_left /etc/audit/auditd.conf  
space_left 250000
```

If the "space_left" parameter is missing, set to blanks, or set to a value less than 25% of the space free in the allocated audit record storage, this is a finding.

If the "space_left_action" parameter is missing or set to blanks, this is a finding.

If the "space_left_action" is set to "syslog", the system logs the event but does not generate a notification, and this is a finding.

If the "space_left_action" is set to "exec", the system executes a designated script. If this script informs the SA of the event, this is not a finding.

If the "space_left_action" is set to "email", check the value of the "action_mail_acct" parameter with the following command:

```
# grep ^action_mail_acct /etc/audit/auditd.conf  
action_mail_acct root@localhost
```

The "action_mail_acct" parameter, if missing, defaults to "root". If the "action_mail_acct" parameter is not set to the email address of the SA(s) and/or ISSO, this is a finding.

Note: If the email address of the System Administrator is on a remote system, a mail package must be available.

Remediation:

Edit "/etc/audit/auditd.conf" and set the "space_left_action" parameter to "exec" or "email".

If the "space_left_action" parameter is set to "email", set the "action_mail_acct" parameter to an email address for the SA and ISSO.

If the "space_left_action" parameter is set to "exec", ensure the command being executed notifies the SA and ISSO.

Edit "/etc/audit/auditd.conf" and set the "space_left" parameter to be at least 25% of the repository maximum audit record storage capacity.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238307
Rule ID: SV-238307r654096_rule
STIG ID: UBTU-20-010217
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.		●	●

4.1.2.8 Ensure crontab script running to offload audit events of standalone systems (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must have a crontab script running weekly to offload audit events of standalone systems.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

Audit:

Note: If this is an interconnected system, this is Not Applicable.

Verify there is a script that offloads audit data and that script runs weekly.

Check if there is a script in the "/etc/cron.weekly" directory that offloads audit data:

```
# ls /etc/cron.weekly  
audit-offload
```

Check if the script inside the file does offloading of audit logs to external media.

If the script file does not exist or does not offload audit logs, this is a finding.

Remediation:

Create a script that offloads audit logs to external media and runs weekly.

The script must be located in the "/etc/cron.weekly" directory.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238321
Rule ID: SV-238321r654138_rule
STIG ID: UBTU-20-010300
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

4.1.3 Configure auditd rules

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 AppArmor 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.

Notes:

- *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*
- *Audit rules that have `archas` a rule parameter:*
 - *On 64 bit systems, you will need two rules, one for 64 bit and one for 32 bit*
 - *On 32 bit systems, only the 32 bit rule is needed*
- *Several recommendations in this section filter based off of `auid>=1000` for unprivileged non-system users. Some systems may have a non-default `UID_MIN` setting, consult the `UID_MIN` setting in `/etc/login.defs` to determine the `UID_MIN` setting for your system*
- *The audits in this section look for a `key` value. The `key` value may be different for the audit rules on your system. If a different `key` value, denoted by `-k` or `key=` is used on your system, please replace the `grep <key_value>` with the `key` value in use on your system*
- *Once all audit rules have been added to a file or files in the `/etc/audit/rules.d/` directory, the `auditd` service must be re-started, or the system rebooted, for the new rules to be included*

4.1.3.1 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"

Note: Reloading the `audited` config to set active settings requires the `audited` service to be restarted, and may require a system reboot.

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:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep time-change /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-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
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep time-change
```

Verify the output matches:

```
-a always,exit -F arch=b32 -S stime,settimofday,adjtimex -F key=time-change  
-a always,exit -F arch=b32 -S clock_settime -F key=time-change  
-w /etc/localtime -p wa -k time-change
```

On a 64 bit system run the following commands:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep time-change /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-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
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep time-change
```

Verify the output matches:

```

-a always,exit -F arch=b64 -S adjtimex,settimoofday -F key=time-change
-a always,exit -F arch=b32 -S stime,settimoofday,adjtimex -F key=time-change
-a always,exit -F arch=b64 -S clock_settime -F key=time-change
-a always,exit -F arch=b32 -S clock_settime -F key=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 settimoofday -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 settimoofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimoofday -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

```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>8.2 Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<u>5.5 Implement Automated Configuration Monitoring Systems</u> 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.		●	●

4.1.3.2 Ensure kernel module loading and unloading is collected (Automated)

Profile Applicability:

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

Description:

Monitor the loading and unloading of kernel modules. The programs `insmod` (install a kernel module), `rmmmod` (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".

Note: Reloading the `auditd` config to set active settings requires the `auditd` service to be restarted, and may require a system reboot.

Rationale:

Monitoring the use of `insmod`, `rmmmod` 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 verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# 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 verify that rules are in the running `auditd` config:

```
# 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 verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# 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 verify that rules are in the running `auditd` config:

```
# 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:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238295
Rule ID: SV-238295r654060_rule
STIG ID: UBTU-20-010179
Severity: CAT II

Vul ID: V-238297
Rule ID: SV-238297r654066_rule
STIG ID: UBTU-20-010181
Severity: CAT II

Vul ID: V-238314
Rule ID: SV-238314r654117_rule
STIG ID: UBTU-20-010276
Severity: CAT II

Vul ID: V-238318
Rule ID: SV-238318r654129_rule
STIG ID: UBTU-20-010296
Severity: CAT II

Vul ID: V-238322
Rule ID: SV-238322r654141_rule
STIG ID: UBTU-20-010302
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.	●	●	●

4.1.3.3 Ensure system administrator command executions (`sudo`) are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

`sudo` provides users with temporary elevated privileges to perform operations. Monitor the administrator with temporary elevated privileges and the operation(s) they performed.

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

Rationale:

Creating an audit log of administrators with temporary elevated privileges and the operation(s) they performed is essential to reporting. Administrators will want to correlate the events written to the audit trail with the records written to `sudo logfile` to verify if unauthorized commands have been executed.

Audit:

On a 32 bit system run the following commands:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep actions /etc/audit/rules.d/*.rules
```

Verify the output includes:

```
-a exit,always -F arch=b32 -C euid!=uid -F euid=0 -F auuid>=1000 -F  
auid!=4294967295 -S execve -k actions
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep actions
```

Verify the output includes:

```
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -F auuid>=1000 -F  
auid!=-1 -F key=actions
```

On a 64 bit system run the following commands:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep actions /etc/audit/rules.d/*.rules
```

Verify the output includes:

```
-a exit,always -F arch=b64 -C euid!=uid -F euid=0 -F auuid>=1000 -F  
auid!=4294967295 -S execve -k actions  
-a exit,always -F arch=b32 -C euid!=uid -F euid=0 -F auuid>=1000 -F  
auid!=4294967295 -S execve -k actions
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep actions
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -F auuid>=1000 -F  
auid!=-1 -F key=actions  
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -F auuid>=1000 -F  
auid!=-1 -F key=actions
```

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-actions.rules`

Add the following line:

```
-a exit,always -F arch=b32 -C euid!=uid -F euid=0 -F auid>=1000 -F  
auid!=4294967295 -S execve -k actions
```

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-actions.rules

Add the following lines:

```
-a always,exit -F arch=b64 -C euid!=uid -F euid=0 -F auid>=1000 -F  
auid!=4294967295 -S execve -k actions  
-a always,exit -F arch=b32 -C euid!=uid -F euid=0 -F auid>=1000 -F  
auid!=4294967295 -S execve -k actions
```

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	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.		●	●

4.1.3.4 Ensure changes to system administration scope (`sudoers`) is collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor scope changes for system administrations. 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."

Note: Reloading the `audited` config to set active settings requires the `audited` service to be restarted, and may require a system reboot.

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 commands:

```
# grep scope /etc/audit/rules.d/*.rules  
# auditctl -l | grep scope
```

Verify output of both 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
```

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	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.		●	●

4.1.3.5 Ensure file deletion events by users are collected (Automated)

Profile Applicability:

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

- 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 requires the auditd service to be restarted, and may require a system reboot.

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 verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# 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 verify that rules are in the running `auditd` config:

```
# auditctl -l | grep delete
```

Verify output matches:

```
-a always,exit -F arch=b32 -S unlink,rename,unlinkat,renameat -F auid>=1000 -  
F auid!=-1 -F key=delete
```

On a 64 bit system run the following commands:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# 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 verify that rules are in the running `auditd` config:

```
# auditctl -l | grep delete
```

Verify output matches:

```
-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F auid>=1000 -  
F auid!=-1 -F key=delete  
-a always,exit -F arch=b32 -S unlink,rename,unlinkat,renameat -F auid>=1000 -  
F auid!=-1 -F key=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-delete.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-delete.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:

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.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238310

Rule ID: SV-238310r654105_rule

STIG ID: UBTU-20-010267

Severity: CAT II

Vul ID: V-238311

Rule ID: SV-238311r654108_rule

STIG ID: UBTU-20-010268

Severity: CAT II

Vul ID: V-238312

Rule ID: SV-238312r654111_rule

STIG ID: UBTU-20-010269

Severity: CAT II

Vul ID: V-238313

Rule ID: SV-238313r654114_rule

STIG ID: UBTU-20-010270

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.	●	●	●

4.1.3.6 Ensure successful file system mounts are collected (Automated)

Profile Applicability:

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

Note:

- 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 requires the `auditd` service to be restarted, and may require a system reboot.

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.

Audit:

On a 32 bit system run the following commands:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# 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 verify that rules are in the running `auditd` config:

```
# auditctl -l | grep mounts
```

Verify output matches:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -F key=mounts
```

On a 64 bit system run the following commands:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# 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 verify that rules are in the running `auditd` config:

```
# auditctl -l | grep mounts
```

Verify output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=-1 -F key=mounts  
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -F key=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:

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.

```
Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 1 Benchmark Date: 10 Mar 2021
```

```
Vul ID: V-238254  
Rule ID: SV-238254r653937_rule  
STIG ID: UBTU-20-010138  
Severity: CAT II
```

```
Vul ID: V-238255  
Rule ID: SV-238255r653940_rule  
STIG ID: UBTU-20-010139  
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.	●	●	●

4.1.3.7 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.

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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>=1000 -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 auid>=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 `key "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:

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.

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.	●	●	●

4.1.3.8 Ensure unsuccessful unauthorized file access attempts are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG - Server
- STIG - 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: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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 verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# 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 verify that rules are in the running `auditd` config:

```
# auditctl -l | grep access
```

Verify output matches:

```
-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat -F exit=-EACCES -F auid>=1000 -F auid!=-1 -F key=access  
-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat -F exit=-EPERM -F auid>=1000 -F auid!=-1 -F key=access
```

On a 64 bit system run the following commands:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# 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 verify that rules are in the running `auditd` config:

```
# auditctl -l | grep access
```

Verify output matches:

```
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit==EACCES -F auid>=1000 -F auid!=--1 -F key=access  
-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat -F exit==EACCES -F auid>=1000 -F auid!=--1 -F key=access  
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit==EPERM -F auid>=1000 -F auid!=--1 -F key=access  
-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat -F exit==EPERM -F auid>=1000 -F auid!=--1 -F key=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:

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.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238271
Rule ID: SV-238271r653988_rule
STIG ID: UBTU-20-010155
Severity: CAT II

Vul ID: V-238272
Rule ID: SV-238272r653991_rule
STIG ID: UBTU-20-010156
Severity: CAT II

Vul ID: V-238273
Rule ID: SV-238273r653994_rule
STIG ID: UBTU-20-010157
Severity: CAT II

Vul ID: V-238274
Rule ID: SV-238274r653997_rule
STIG ID: UBTU-20-010158
Severity: CAT II

Vul ID: V-238275
Rule ID: SV-238275r654000_rule
STIG ID: UBTU-20-010159
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>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).</p>			●

4.1.3.9 Ensure discretionary access control permission modification events are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG - Server
- STIG - 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: Reloading the `auditd` config to set active settings requires the `auditd` service to be restarted, and may require a system reboot.

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 verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# 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 verify that rules are in the running `auditd` config:

```
# 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 verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# 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 verify that rules are in the running `auditd` config:

```
# 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:

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.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238264
Rule ID: SV-238264r653967_rule
STIG ID: UBTU-20-010148
Severity: CAT II

Vul ID: V-238265
Rule ID: SV-238265r653970_rule
STIG ID: UBTU-20-010149
Severity: CAT II

Vul ID: V-238266
Rule ID: SV-238266r653973_rule
STIG ID: UBTU-20-010150
Severity: CAT II

Vul ID: V-238267
Rule ID: SV-238267r653976_rule
STIG ID: UBTU-20-010151
Severity: CAT II

Vul ID: V-238268
Rule ID: SV-238268r653979_rule
STIG ID: UBTU-20-010152
Severity: CAT II

Vul ID: V-238269
Rule ID: SV-238269r653982_rule
STIG ID: UBTU-20-010153
Severity: CAT II

Vul ID: V-238270
Rule ID: SV-238270r653985_rule
STIG ID: UBTU-20-010154
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>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.</p>		●	●
v7	<p>6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●

4.1.3.10 Ensure session initiation information is collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG - Server
- STIG - 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."

Note:

- 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 requires the auditd service to be restarted, and may require a system reboot.

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 verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# 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 verify that rules are in the running `auditd` config:

```
# 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:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238315

Rule ID: SV-238315r654120_rule

STIG ID: UBTU-20-010277

Severity: CAT II

Vul ID: V-238316

Rule ID: SV-238316r654123_rule

STIG ID: UBTU-20-010278

Severity: CAT II

Vul ID: V-238317

Rule ID: SV-238317r654126_rule

STIG ID: UBTU-20-010279

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>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.</p>		●	●
v7	<p>6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p>16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.</p>	●	●	●
v7	<p>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.</p>			●

4.1.3.11 Ensure login and logout events are collected (Automated)

Profile Applicability:

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

Description:

Monitor login and logout events. The parameters below track changes to files associated with login/logout events. The file `/var/log/faillog` tracks failed events from login. The file `/var/log/lastlog` maintains records of the last time a user successfully logged in. The file `/var/log/tallylog` maintains records of failures via the `pam_tally2` module.

Note: Reloading the `auditd` config to set active settings requires the `auditd` service to be restarted, and may require a system reboot.

Rationale:

Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Audit:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep logins /etc/audit/rules.d/*.rules
```

Verify output includes:

```
-w /var/log/faillog -p wa -k logins  
-w /var/log/lastlog -p wa -k logins  
-w /var/log/tallylog -p wa -k logins
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep logins
```

Verify output includes:

```
-w /var/log/faillog -p wa -k logins  
-w /var/log/lastlog -p wa -k logins  
-w /var/log/tallylog -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/faillog -p wa -k logins  
-w /var/log/lastlog -p wa -k logins  
-w /var/log/tallylog -p wa -k logins
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238285
Rule ID: SV-238285r654030_rule
STIG ID: UBTU-20-010169
Severity: CAT II

Vul ID: V-238286
Rule ID: SV-238286r654033_rule
STIG ID: UBTU-20-010170
Severity: CAT II

Vul ID: V-238287
Rule ID: SV-238287r654036_rule
STIG ID: UBTU-20-010171
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	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	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●
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.			●

4.1.3.12 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor 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 `/etc/apparmor` and `/etc/apparmor.d` directories.

Note: Reloading the `audited` config to set active settings requires the `auditd` service to be restarted, and may require a system reboot.

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 command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep MAC-policy /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-w /etc/apparmor/ -p wa -k MAC-policy  
-w /etc/apparmor.d/ -p wa -k MAC-policy
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep MAC-policy
```

Verify output matches:

```
-w /etc/apparmor/ -p wa -k MAC-policy  
-w /etc/apparmor.d/ -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/apparmor/ -p wa -k MAC-policy  
-w /etc/apparmor.d/ -p wa -k MAC-policy
```

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	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.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.3.13 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/network` (directory containing network interface scripts and configurations) files.

Note: Reloading the `audited` config to set active settings requires the `audited` service to be restarted, and may require a system reboot.

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/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:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep system-locale /etc/audit/rules.d/*.rules
```

Verify the output 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/network -p wa -k system-locale
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep system-locale
```

Verify the output matches:

```
-a always,exit -F arch=b32 -S sethostname,setdomainname -F key=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/network -p wa -k system-locale
```

On a 64 bit system run the following commands:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep system-locale /etc/audit/rules.d/*.rules
```

Verify the output 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/network -p wa -k system-locale
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep system-locale
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S sethostname,setdomainname -F key=system-locale  
-a always,exit -F arch=b32 -S sethostname,setdomainname -F key=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/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-locale.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/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-locale.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/network -p wa -k system-locale
```

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>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.</p>		●	●
v7	<p>6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●

4.1.3.14 Ensure events that modify user/group information are collected (Automated)

Profile Applicability:

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

Note: Reloading the `audited` config to set active settings requires the `audited` service to be restarted, and may require a system reboot.

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 verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# 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 verify that rules are in the running `auditd` config:

```
# 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:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238238
Rule ID: SV-238238r653889_rule
STIG ID: UBTU-20-010100
Severity: CAT II

Vul ID: V-238239
Rule ID: SV-238239r653892_rule
STIG ID: UBTU-20-010101
Severity: CAT II

Vul ID: V-238240
Rule ID: SV-238240r653895_rule
STIG ID: UBTU-20-010102
Severity: CAT II

Vul ID: V-238241
Rule ID: SV-238241r653898_rule
STIG ID: UBTU-20-010103
Severity: CAT II

Vul ID: V-238242
Rule ID: SV-238242r653901_rule
STIG ID: UBTU-20-010104
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	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.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.1.3.15 Ensure successful and unsuccessful uses of the su command are collected (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the su command.

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).

Audit:

Verify the Ubuntu operating system generates audit records upon successful/unsuccessful attempts to use the "su" command.

Check the configured audit rules with the following commands:

```
# auditctl -l | grep '/bin/su'  
-a always,exit -F path=/bin/su -F perm=x -F auid>=1000 -F auid!=4294967295 -k  
privileged-priv_change
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the Ubuntu operating system to generate audit records when successful/unsuccessful attempts to use the "su" command occur.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/bin/su -F perm=x -F auid>=1000 -F auid!=4294967295 -k  
privileged-priv_change
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238252
Rule ID: SV-238252r653931_rule
STIG ID: UBTU-20-010136
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.	●	●	●

4.1.3.16 Ensure successful and unsuccessful uses of the chfn command are collected (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the chfn command.

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).

Audit:

Verify the Ubuntu operating system generates audit records upon successful/unsuccessful attempts to use the "chfn" command.

Check the configured audit rules with the following commands:

```
# auditctl -l | grep '/usr/bin/chfn'  
-a always,exit -F path=/usr/bin/chfn -F perm=x -F auid>=1000 -F auid!=--1 -k  
privileged-chfn
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "chfn" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/chfn -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k privileged-chfn
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238253
Rule ID: SV-238253r653934_rule
STIG ID: UBTU-20-010137
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.	●	●	●

4.1.3.17 Ensure successful and unsuccessful uses of the ssh-agent command are collected (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the ssh-agent command.

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).

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "ssh-agent" command.
Check the configured audit rules with the following commands:

```
# auditctl -l | grep '/usr/bin/ssh-agent'  
-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F auid!=-1  
-k privileged-ssh
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "ssh-agent" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k privileged-ssh
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238256
Rule ID: SV-238256r653943_rule
STIG ID: UBTU-20-010140
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.	●	●	●

4.1.3.18 Ensure successful and unsuccessful uses of the ssh-keysign command are collected (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the ssh-keysign command.

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).

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "ssh-keysign" command.

Check the configured audit rules with the following commands:

```
# auditctl -l | grep ssh-keysign  
-a always,exit -F path=/usr/lib/openssh/ssh-keysign -F perm=x -F auid>=1000 -  
F auid!=--1 -k privileged-ssh
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "ssh-keysign" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/lib/openssh/ssh-keysign -F perm=x -F auid>=1000 -  
F auid!=4294967295 -k privileged-ssh
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238257
Rule ID: SV-238257r653946_rule
STIG ID: UBTU-20-010141
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.	●	●	●

4.1.3.19 Ensure successful and unsuccessful attempts to use the setxattr system call are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for any use 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).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the `setxattr` system call.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep setxattr  
  
-a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=-1 -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>=1000 -F auid!=-1 -k perm_mod  
-a always,exit -F arch=b64 -S setxattr -F auid=0 -k perm_mod
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Notes:

- For 32-bit architectures, only the 32-bit specific output lines from the commands are required.
- The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "setxattr" system call.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=4294967295 -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>=1000 -F auid!=4294967295 -k perm_mod  
-a always,exit -F arch=b64 -S setxattr -F auid=0 -k perm_mod
```

Notes: For 32-bit architectures, only the 32-bit specific entries are required.

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238258
Rule ID: SV-238258r653949_rule
STIG ID: UBTU-20-010142
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.	●	●	●

4.1.3.20 Ensure successful and unsuccessful attempts to use the lsetxattr system call are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for any use 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).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "lsetxattr" system call.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep lsetxattr  
  
-a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=--1 -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>=1000 -F auid!=--1 -k perm_mod  
-a always,exit -F arch=b64 -S lsetxattr -F auid=0 -k perm_mod
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Notes:

- For 32-bit architectures, only the 32-bit specific output lines from the commands are required.
- The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "lsetxattr" system call.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=--1 -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>=1000 -F auid!=--1 -k perm_mod  
-a always,exit -F arch=b64 -S lsetxattr -F auid=0 -k perm_mod
```

Notes: For 32-bit architectures, only the 32-bit specific entries are required.

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238259

Rule ID: SV-238259r653952 rule

STIG ID: UBTU-20-010143

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.	●	●	●

4.1.3.21 Ensure successful and unsuccessful attempts to use the fsetxattr system call are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for any use 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).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "fsetxattr" system call.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep fsetxattr  
  
-a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=--1 -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>=1000 -F auid!=--1 -k perm_mod  
-a always,exit -F arch=b64 -S fsetxattr -F auid=0 -k perm_mod
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Notes:

- For 32-bit architectures, only the 32-bit specific output lines from the commands are required.
- The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "fsetxattr" system call.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=4294967295 -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>=1000 -F auid!=4294967295 -k perm_mod  
-a always,exit -F arch=b64 -S fsetxattr -F auid=0 -k perm_mod
```

Notes: For 32-bit architectures, only the 32-bit specific entries are required.

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238260
Rule ID: SV-238260r653955_rule
STIG ID: UBTU-20-010144
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.	●	●	●

4.1.3.22 Ensure successful and unsuccessful attempts to use the removexattr system call are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for any use 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).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "removexattr" system call.
Check the currently configured audit rules with the following command:

```
# auditctl -l | grep removexattr  
  
-a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=--1 -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>=1000 -F auid!=--1 -k  
perm_mod  
-a always,exit -F arch=b64 -S removexattr -F auid=0 -k perm_mod
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Notes:

- For 32-bit architectures, only the 32-bit specific output lines from the commands are required.
- The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "removexattr" system call.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=4294967295 -  
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>=1000 -F auid!=4294967295 -  
k perm_mod  
-a always,exit -F arch=b64 -S removexattr -F auid=0 -k perm_mod
```

Notes: For 32-bit architectures, only the 32-bit specific entries are required.

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238261
Rule ID: SV-238261r653958_rule
STIG ID: UBTU-20-010145
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.	●	●	●

4.1.3.23 Ensure successful and unsuccessful attempts to use the fremoveattr system call are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for any use of the `fremoveattr` 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).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000365-GPOS-00152

Audit:

Verify if the Ubuntu operating system is configured to audit the execution of the "fremovexattr" system call.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep fremovexattr  
  
-a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=-1 -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>=1000 -F auid!=-1 -k  
perm_mod  
-a always,exit -F arch=b64 -S fremovexattr -F auid=0 -k perm_mod
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Notes:

- For 32-bit architectures, only the 32-bit specific output lines from the commands are required.
- The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "fremovexattr" system call.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=4294967295  
-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>=1000 -F auid!=4294967295  
-k perm_mod  
-a always,exit -F arch=b64 -S fremovexattr -F auid=0 -k perm_mod
```

Notes: For 32-bit architectures, only the 32-bit specific entries are required.

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238263
Rule ID: SV-238263r653964_rule
STIG ID: UBTU-20-010147
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.	●	●	●

4.1.3.24 Ensure successful and unsuccessful attempts to use the lremovexattr system call are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for any use 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).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210

Audit:

Verify if the Ubuntu operating system is configured to audit the execution of the "lremovexattr" system call.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep lremovexattr  
  
-a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=--1 -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>=1000 -F auid!=--1 -k  
perm_mod  
-a always,exit -F arch=b64 -S lremovexattr -F auid=0 -k perm_mod
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Notes:

- For 32-bit architectures, only the 32-bit specific output lines from the commands are required.
- The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "lremovexattr" system call.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=4294967295  
-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>=1000 -F auid!=4294967295  
-k perm_mod  
-a always,exit -F arch=b64 -S lremovexattr -F auid=0 -k perm_mod
```

Notes: For 32-bit architectures, only the 32-bit specific entries are required.

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238262
Rule ID: SV-238262r653961_rule
STIG ID: UBTU-20-010146
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.	●	●	●

4.1.3.25 Ensure successful and unsuccessful uses of the open_by_handle_at system call are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the open_by_handle_at 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).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000474-GPOS-00219

Audit:

Verify the Ubuntu operating system generates an audit record upon unsuccessful attempts to use the "open_by_handle_at" system call.

Check the configured audit rules with the following command:

```
# auditctl -l | grep open_by_handle_at

-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EPERM -F auid>=1000
-F auid!=4294967295 -k perm_access
-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EACCES -F auid>=1000
-F auid!=4294967295 -k perm_access
-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EPERM -F auid>=1000
-F auid!=4294967295 -k perm_access
-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EACCES -F auid>=1000
-F auid!=4294967295 -k perm_access
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Notes:

- For 32-bit architectures, only the 32-bit specific output lines from the commands are required.
- The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any unsuccessful use of the "open_by_handle_at" system call.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EPERM -F auid>=1000
-F auid!=4294967295 -k perm_access
-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EACCES -F auid>=1000
-F auid!=4294967295 -k perm_access
-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EPERM -F auid>=1000
-F auid!=4294967295 -k perm_access
-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EACCES -F auid>=1000
-F auid!=4294967295 -k perm_access
```

Notes: For 32-bit architectures, only the 32-bit specific entries are required.

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238276
Rule ID: SV-238276r654003_rule
STIG ID: UBTU-20-010160
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.	●	●	●

4.1.3.26 Ensure successful and unsuccessful uses of the sudo command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the sudo command.

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).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "sudo" command.

Check the configured audit rules with the following command:

```
# auditctl -l | grep /usr/bin/sudo  
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=--1 -k  
priv_cmd
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "sudo" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k priv_cmd
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238277
Rule ID: SV-238277r654006_rule
STIG ID: UBTU-20-010161
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.	●	●	●

4.1.3.27 Ensure successful and unsuccessful attempts to use the sudoedit command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the sudoedit command.

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).

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "sudoedit" command.

Check the configured audit rules with the following commands:

```
# auditctl -l | grep /usr/bin/sudoedit  
-a always,exit -F path=/usr/bin/sudoedit -F perm=x -F auid>=1000 -F auid!=--1  
-k priv_cmd
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "sudoedit" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules":

```
-a always,exit -F path=/usr/bin/sudoedit -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k priv_cmd
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238278
Rule ID: SV-238278r654009_rule
STIG ID: UBTU-20-010162
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.	●	●	●

4.1.3.28 Ensure successful and unsuccessful attempts to use the chsh command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the chsh command.

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).

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "chsh" command.

Check the configured audit rules with the following commands:

```
# auditctl -l | grep chsh  
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=--1 -k  
priv_cmd
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chsh" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k priv_cmd
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238279
Rule ID: SV-238279r654012_rule
STIG ID: UBTU-20-010163
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.	●	●	●

4.1.3.29 Ensure successful and unsuccessful attempts to use the newgrp command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the newgrp command.

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).

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "newgrp" command.

Check the configured audit rules with the following commands:

```
# auditctl -l | grep newgrp  
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=--1 -k  
priv_cmd
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "newgrp" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k priv_cmd
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238280
Rule ID: SV-238280r654015_rule
STIG ID: UBTU-20-010164
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.	●	●	●

4.1.3.30 Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the chcon command.

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).

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "chcon" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep chcon  
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k perm_chng
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chcon" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k perm_chng
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238281
Rule ID: SV-238281r654018_rule
STIG ID: UBTU-20-010165
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.	●	●	●

4.1.3.31 Ensure successful and unsuccessful attempts to use the apparmor_parser command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the apparmor_parser command.

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).

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "apparmor_parser" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep apparmor_parser  
-a always,exit -F path=/sbin/apparmor_parser -F perm=x -F auid>=1000 -F  
auid!=--1 -k perm_chng
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "apparmor_parser" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/sbin/apparmor_parser -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k perm_chng
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238282
Rule ID: SV-238282r654021_rule
STIG ID: UBTU-20-010166
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.	●	●	●

4.1.3.32 Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the setfacl command

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).

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "setfacl" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep setfacl  
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F auid!==1 -  
k perm_chng
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "setfacl" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k perm_chng
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238283
Rule ID: SV-238283r654024_rule
STIG ID: UBTU-20-010167
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.	●	●	●

4.1.3.33 Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the chacl command

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).

Audit:

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "chacl" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep chacl  
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=--1 -k  
perm_chng
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chacl" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k perm_chng
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238284
Rule ID: SV-238284r654027_rule
STIG ID: UBTU-20-010168
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.	●	●	●

4.1.3.34 Ensure successful and unsuccessful attempts to use the passwd command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the passwd command

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).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "passwd" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w passwd  
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=-1 -k  
privileged-passwd
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "passwd" command.

Add or update the following rule in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k privileged-passwd
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238288
Rule ID: SV-238288r654039_rule
STIG ID: UBTU-20-010172
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.	●	●	●

4.1.3.35 Ensure successful and unsuccessful attempts to use the unix_update command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the unix_update command

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).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "unix_update" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w unix_update  
-a always,exit -F path=/sbin/unix_update -F perm=x -F auid>=1000 -F auid!=--1  
-k privileged-unix-update
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "unix_update" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/sbin/unix_update -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k privileged-unix-update
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238289
Rule ID: SV-238289r654042_rule
STIG ID: UBTU-20-010173
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.	●	●	●

4.1.3.36 Ensure successful and unsuccessful attempts to use the gpasswd command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the gpasswd command

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).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "gpasswd" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w gpasswd  
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F auid!=-1 -  
k privileged-gpasswd
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "gpasswd" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k privileged-gpasswd
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238290
Rule ID: SV-238290r654045_rule
STIG ID: UBTU-20-010174
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.	●	●	●

4.1.3.37 Ensure successful and unsuccessful attempts to use the chage command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the chage command

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).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "chage" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w chage  
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=--1 -k  
privileged-chage
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "chage" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k privileged-chage
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238291
Rule ID: SV-238291r654048_rule
STIG ID: UBTU-20-010175
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.	●	●	●

4.1.3.38 Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the usermod command.

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).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "usermod" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w usermod  
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F auid!=--1  
-k privileged-usermod
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "usermod" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k privileged-usermod
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238292
Rule ID: SV-238292r654051_rule
STIG ID: UBTU-20-010176
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.	●	●	●

4.1.3.39 Ensure successful and unsuccessful attempts to use the crontab command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the crontab command.

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).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "crontab" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w crontab  
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F auid!=-1 -  
k privileged-crontab
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "crontab" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k privileged-crontab
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238293
Rule ID: SV-238293r654054_rule
STIG ID: UBTU-20-010177
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.	●	●	●

4.1.3.40 Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the pam_timestamp_check command.

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).

Audit:

Verify that an audit event is generated for any successful/unsuccessful use of the "pam_timestamp_check" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w pam_timestamp_check  
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000  
-F auid!=--1 -k privileged-pam_timestamp_check
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "pam_timestamp_check" command.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000  
-F auid!=4294967295 -k privileged-pam_timestamp_check
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238294
Rule ID: SV-238294r654057_rule
STIG ID: UBTU-20-010178
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.	●	●	●

4.1.3.41 Ensure successful and unsuccessful uses of the `fini_module` syscall are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the `fini_module` syscall.

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-000064-GPOS-00033, SRG-OS-000477-GPOS-00222

Audit:

Verify the Ubuntu operating system generates an audit record for any successful/unsuccessful attempts to use the "finit_module" syscall.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w finit_module  
  
-a always,exit -F arch=b32 -S finit_module -F auid>=1000 -F auid!=-1 -k  
module_chng  
-a always,exit -F arch=b64 -S finit_module -F auid>=1000 -F auid!=-1 -k  
module_chng
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

Notes:

- For 32-bit architectures, only the 32-bit specific output lines from the commands are required.
- The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "finit_module" syscall.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b32 -S finit_module -F auid>=1000 -F auid!=4294967295  
-k module_chng  
-a always,exit -F arch=b64 -S finit_module -F auid>=1000 -F auid!=4294967295  
-k module_chng
```

Notes: For 32-bit architectures, only the 32-bit specific entries are required.

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238296
Rule ID: SV-238296r654063_rule
STIG ID: UBTU-20-010180
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.	●	●	●

4.1.3.42 Ensure execution of privileged functions is recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must prevent all software from executing at higher privilege levels than users executing the software and the audit system must be configured to audit the execution of privileged functions.

Rationale:

In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by the organizations.

Some programs and processes are required to operate at a higher privilege level and therefore should be excluded from the organization-defined software list after review.

Satisfies: SRG-OS-000326-GPOS-00126, SRG-OS-000327-GPOS-00127

Audit:

Verify the Ubuntu operating system audits the execution of privilege functions by auditing the "execve" system call.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep execve  
  
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -F key=execpriv  
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -F key=execpriv  
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -F key=execpriv  
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -F key=execpriv
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

****Notes:**

- For 32-bit architectures, only the 32-bit specific output lines from the commands are required.
- The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the Ubuntu operating system to audit the execution of all privileged functions.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -F key=execpriv  
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -F key=execpriv  
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -F key=execpriv  
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -F key=execpriv
```

Notes: For 32-bit architectures, only the 32-bit specific entries are required.

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238304
Rule ID: SV-238304r654087_rule
STIG ID: UBTU-20-010211
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.	●	●	●

4.1.3.43 Ensure nonlocal administrative access events are collected (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records for privileged activities, nonlocal maintenance, diagnostic sessions and other system-level access.

Rationale:

If events associated with nonlocal administrative access or diagnostic sessions are not logged, a major tool for assessing and investigating attacks would not be available.

This requirement addresses auditing-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

This requirement applies to hardware/software diagnostic test equipment or tools. This requirement does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch.

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Audit:

Verify the Ubuntu operating system audits activities performed during nonlocal maintenance and diagnostic sessions.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep sudo.log  
-w /var/log/sudo.log -p wa -k maintenance
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the Ubuntu operating system to audit activities performed during nonlocal maintenance and diagnostic sessions.

Add or update the following rules in the "/etc/audit/rules.d/stig.rules" file:

```
-w /var/log/sudo.log -p wa -k maintenance
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

```
Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 1 Benchmark Date: 10 Mar 2021
```

```
Vul ID: V-238309  
Rule ID: SV-238309r654102_rule  
STIG ID: UBTU-20-010244  
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.	●	●	●

4.1.3.44 Ensure successful and unsuccessful attempts to use the kmod command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records when successful/unsuccessful attempts to use the kmod command.

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).

Audit:

Verify the Ubuntu operating system is configured to audit the execution of the module management program "kmod".

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep kmod  
-w /bin/kmod -p x -k module
```

If the command does not return a line, or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the Ubuntu operating system to audit the execution of the module management program "kmod".

Add or update the following rule in the "/etc/audit/rules.d/stig.rules" file:

```
-w /bin/kmod -p x -k modules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238319
Rule ID: SV-238319r654132_rule
STIG ID: UBTU-20-010297
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.	●	●	●

4.1.3.45 Ensure successful and unsuccessful attempts to use the fdisk command are recorded (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must generate audit records when successful/unsuccessful attempts to use the fdisk command.

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).

Audit:

Verify the Ubuntu operating system is configured to audit the execution of the module management program "fdisk".

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep fdisk  
-w /bin/fdisk -p x -k module
```

If the command does not return a line, or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the Ubuntu operating system to audit the execution of the partition management program "fdisk".

Add or update the following rule in the "/etc/audit/rules.d/stig.rules" file:

```
-w /bin/fdisk -p x -k fdisk
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238320
Rule ID: SV-238320r654135_rule
STIG ID: UBTU-20-010298
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.	●	●	●

4.1.3.46 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.

Note: Reloading the `audited` config to set active settings requires the `audited` service to be restarted, and may require a 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 line

```
-e 2
```

at the end of the file

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>		●	●

4.1.4 Configure auditd file access

Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events.

4.1.4.1 Ensure audit log files are not read or write-accessible by unauthorized users (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must be configured so that audit log files are not read or write-accessible by unauthorized users.

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 operating system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028

Audit:

Verify that the audit log files have a mode of "0600" or less permissive.
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 path of the directory containing the audit logs, determine if the audit log files have a mode of "0600" or less by using the following command:

```
# stat -c "%n %a" /var/log/audit/*  
/var/log/audit/audit.log 600
```

If the audit log files have a mode more permissive than "0600", this is a finding.

Remediation:

Configure the audit log files to have a mode of "0600" or less permissive. 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 path of the directory containing the audit logs, configure the audit log files to have a mode of "0600" or less permissive by using the following command:

```
# chmod 0600 /var/log/audit/*
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238245
Rule ID: SV-238245r653910_rule
STIG ID: UBTU-20-010122
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.	●	●	●

4.1.4.2 Ensure only authorized users own audit log files (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must be configured to permit only authorized users ownership of the audit log files.

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 operating system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit log files are owned by "root" account.

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 path of the directory containing the audit logs, determine if the audit log files are owned by the "root" user by using the following command:

```
# stat -c "%n %U" /var/log/audit/*  
/var/log/audit/audit.log root
```

If the audit log files are owned by an user other than "root", this is a finding.

Remediation:

Configure the audit log directory and its underlying files to be owned by "root" user.
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 path of the directory containing the audit logs, configure the audit log files to be owned by "root" user by using the following command:

```
# chown root /var/log/audit/*
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238246
Rule ID: SV-238246r653913_rule
STIG ID: UBTU-20-010123
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.	●	●	●

4.1.4.3 Ensure only authorized groups ownership of audit log files (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must permit only authorized groups ownership of the audit log files.

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 operating system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the group owner is set to own newly created audit logs in the audit configuration file with the following command:

```
# grep -iw log_group /etc/audit/auditd.conf  
log_group = adm
```

If the value of the "log_group" parameter is other than "root" or "adm", this is a finding. Determine where the audit logs are stored with the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf  
log_file = /var/log/audit/audit.log
```

Using the path of the directory containing the audit logs, determine if the audit log files are owned by the "root" or "adm" group by using the following command:

```
# stat -c "%n %G" /var/log/audit/*  
/var/log/audit/audit.log root
```

If the audit log files are owned by a group other than "root" or "adm", this is a finding.

Remediation:

Configure the audit log directory and its underlying files to be owned by "adm" group.
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 path of the directory containing the audit logs, configure the audit log files to be owned by "adm" group by using the following command:

```
# chown :adm /var/log/audit/
```

Set the "log_group" parameter of the audit configuration file to the "adm" value so that when a new log file is created, its group owner is properly set:

```
# sed -i '/^log_group/D' /etc/audit/auditd.conf  
# sed -i '/^log_file/a'log_group = adm' /etc/audit/auditd.conf
```

Last, signal the audit daemon to reload the configuration file:

```
# systemctl kill auditd -s SIGHUP"
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238247
Rule ID: SV-238247r653916_rule
STIG ID: UBTU-20-010124
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	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
	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.			

4.1.4.4 Ensure the audit log directory is 0750 or more restrictive (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must be configured so that the audit log directory is not write-accessible by unauthorized users.

Rationale:

If audit information were to become compromised, then forensic analysis and discovery of the true source of potentially malicious system activity is impossible to achieve.

To ensure the veracity of audit information, the operating system must protect audit information from unauthorized deletion. This requirement can be achieved through multiple methods, which will depend upon system architecture and design.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit information system activity.

Audit:

Verify that the audit log directory has a mode of 0750 or less permissive.
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 path of the directory containing the audit logs, determine if the directory has a mode of "0750" or less by using the following command:

```
# stat -c "%n %a" /var/log/audit /var/log/audit/*
/var/log/audit 750
/var/log/audit/audit.log 600
```

If the audit log directory has a mode more permissive than 0750, this is a finding.

Remediation:

Configure the audit log directory to have a mode of "0750" or less permissive.
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 path of the directory containing the audit logs, configure the audit log directory to have a mode of "0750" or less permissive by using the following command:

```
# chmod -R g-w,o-rwx /var/log/audit
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238248
Rule ID: SV-238248r653919_rule
STIG ID: UBTU-20-010128
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.	●	●	●

4.1.4.5 Ensure audit configuration files are 0640 or more restrictive (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must be configured so that audit configuration files are not write-accessible by unauthorized users.

Rationale:

Without the capability to restrict which roles and individuals 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 "/etc/audit/audit.rules", "/etc/audit/rules.d/*", and "/etc/audit/auditd.conf" files have a mode of "0640" or less permissive by using the following command:

```
# ls -al /etc/audit/ /etc/audit/rules.d/  
  
/etc/audit/:  
-rw-r----- 1 root root 804 Nov 25 11:01 auditd.conf  
-rw-r----- 1 root root 9128 Dec 27 09:56 audit.rules  
-rw-r----- 1 root root 9373 Dec 27 09:56 audit.rules.prev  
-rw-r----- 1 root root 127 Feb 7 2018 audit-stop.rules  
drwxr-x--- 2 root root 4096 Dec 27 09:56 rules.d  
  
/etc/audit/rules.d/:  
-rw-r----- 1 root root 10357 Dec 27 09:56 stig.rules
```

If "/etc/audit/audit.rule", "/etc/audit/rules.d/*", or "/etc/audit/auditd.conf" file have a mode more permissive than "0640", this is a finding.

Remediation:

Configure "/etc/audit/audit.rules", "/etc/audit/rules.d/*", and "/etc/audit/auditd.conf" files to have a mode of "0640" by using the following command:

```
# chmod -R 0640 /etc/audit/audit*.{rules,conf} /etc/audit/rules.d/*
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238249
Rule ID: SV-238249r653922_rule
STIG ID: UBTU-20-010133
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.	●	●	●

4.1.4.6 Ensure only authorized accounts own the audit configuration files (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must permit only authorized accounts to own the audit configuration files.

Rationale:

Without the capability to restrict which roles and individuals 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 "/etc/audit/audit.rules", "/etc/audit/rules.d/*" and "/etc/audit/auditd.conf" files are owned by root account by using the following command:

```
# ls -al /etc/audit/ /etc/audit/rules.d/  
  
/etc/audit/:  
drwxr-x--- 3 root root 4096 Nov 25 11:02 .  
drwxr-xr-x 130 root root 12288 Dec 19 13:42 ..  
-rw-r----- 1 root root 804 Nov 25 11:01 auditd.conf  
-rw-r----- 1 root root 9128 Dec 27 09:56 audit.rules  
-rw-r----- 1 root root 9373 Dec 27 09:56 audit.rules.prev  
-rw-r----- 1 root root 127 Feb 7 2018 audit-stop.rules  
drwxr-x--- 2 root root 4096 Dec 27 09:56 rules.d  
  
/etc/audit/rules.d/:  
drwxr-x--- 2 root root 4096 Dec 27 09:56 .  
drwxr-x--- 3 root root 4096 Nov 25 11:02 ..  
-rw-r----- 1 root root 10357 Dec 27 09:56 stig.rules
```

If the "/etc/audit/audit.rules", "/etc/audit/rules.d/*", or "/etc/audit/auditd.conf" file is owned by a user other than "root", this is a finding.

Remediation:

Configure "/etc/audit/audit.rules", "/etc/audit/rules.d/*" and "/etc/audit/auditd.conf" files to be owned by root user by using the following command:

```
# chown root /etc/audit/audit*.{rules,conf} /etc/audit/rules.d/*
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238250
Rule ID: SV-238250r653925_rule
STIG ID: UBTU-20-010134
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.	●	●	●

4.1.4.7 Ensure only authorized groups own the audit configuration files (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must permit only authorized groups to own the audit configuration files.

Rationale:

Without the capability to restrict which roles and individuals 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 "/etc/audit/audit.rules", "/etc/audit/rules.d/*", and "/etc/audit/auditd.conf" files are owned by root group by using the following command:

```
# ls -al /etc/audit/ /etc/audit/rules.d/  
  
/etc/audit/:  
-rw-r----- 1 root root 804 Nov 25 11:01 auditd.conf  
-rw-r----- 1 root root 9128 Dec 27 09:56 audit.rules  
-rw-r----- 1 root root 9373 Dec 27 09:56 audit.rules.prev  
-rw-r----- 1 root root 127 Feb 7 2018 audit-stop.rules  
drwxr-x--- 2 root root 4096 Dec 27 09:56 rules.d  
  
/etc/audit/rules.d/:  
-rw-r----- 1 root root 10357 Dec 27 09:56 stig.rules
```

If the "/etc/audit/audit.rules", "/etc/audit/rules.d/*", or "/etc/audit/auditd.conf" file is owned by a group other than "root", this is a finding.

Remediation:

Configure "/etc/audit/audit.rules", "/etc/audit/rules.d/*", and "/etc/audit/auditd.conf" files to be owned by root group by using the following command:

```
# chown :root /etc/audit/audit*.{rules,conf} /etc/audit/rules.d/*
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238251
Rule ID: SV-238251r653928_rule
STIG ID: UBTU-20-010135
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.	●	●	●

4.1.4.8 Ensure audit tools are mode of 0755 or more restrictive (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must configure audit tools with 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.

Operating 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 in order 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

Audit:

Verify the Ubuntu operating system configures the audit tools to have a file permission of 0755 or less to prevent unauthorized access by running the following command:

```
# stat -c "%n %a" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/audispd /sbin/augenrules  
  
/sbin/auditctl 755  
/sbin/aureport 755  
/sbin/ausearch 755  
/sbin/autrace 755  
/sbin/auditd 755  
/sbin/audispd 755  
/sbin/augenrules 755
```

If any of the audit tools have a mode more permissive than 0755, this is a finding.

Remediation:

Configure the audit tools on the Ubuntu operating system 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 permissions.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238300
Rule ID: SV-238300r654075_rule
STIG ID: UBTU-20-010199
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.	●	●	●

4.1.4.9 Ensure audit tools are owned by root (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must configure audit tools to 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.

Operating 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 in order 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

Audit:

Verify the Ubuntu operating system configures the audit tools to be owned by root to prevent any unauthorized access.

Check the ownership by running the following command:

```
# stat -c "%n %U" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/audispd /sbin/augenrules  
  
/sbin/auditctl root  
/sbin/aureport root  
/sbin/ausearch root  
/sbin/autrace root  
/sbin/auditd root  
/sbin/audispd root  
/sbin/augenrules root
```

If any of the audit tools are not owned by root, this is a finding.

Remediation:

Configure the audit tools on the Ubuntu operating system to be protected from unauthorized access by setting the file owner as root using the following command:

```
# chown root [audit_tool]
```

Replace "[audit_tool]" with each audit tool not owned by root.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238301
Rule ID: SV-238301r654078_rule
STIG ID: UBTU-20-010200
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.	●	●	●

4.1.4.10 Ensure audit tools are group-owned by root (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must configure the audit tools to 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.

Operating 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 in order 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

Audit:

Verify the Ubuntu operating system configures the audit tools to be group-owned by root to prevent any unauthorized access.

Check the group ownership by running the following command:

```
# stat -c "%n %G" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/audispd /sbin/augenrules  
  
/sbin/auditctl root  
/sbin/aureport root  
/sbin/ausearch root  
/sbin/autrace root  
/sbin/auditd root  
/sbin/audispd root  
/sbin/augenrules root
```

If any of the audit tools are not owned by root, this is a finding.

Remediation:

Configure the audit tools on the Ubuntu operating system to be protected from unauthorized access by setting the file group as root using the following command:

```
# chown :root [audit_tool]
```

Replace "[audit_tool]" with each audit tool not group-owned by root.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238302
Rule ID: SV-238302r654081_rule
STIG ID: UBTU-20-010201
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.	●	●	●

4.1.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

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 in order 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.

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

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

/sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/audispd p+i+n+u+g+s+b+acl+xattrs+sha512
/sbin/augenrules p+i+n+u+g+s+b+acl+xattrs+sha512
```

If any of the seven audit tools do not have appropriate selection lines, this is a finding.

Remediation:

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

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

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238303
Rule ID: SV-238303r654084_rule
STIG ID: UBTU-20-010205
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.	●	●	●

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.

4.2.1.1 Ensure rsyslog is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG - Server
- STIG - 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 either `rsyslog` or `syslog-ng` is installed. Use the following command to provide the needed information:

```
# dpkg -s rsyslog
```

Remediation:

Install `rsyslog`:

```
# apt install rsyslog
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238353
Rule ID: SV-238353r654234_rule
STIG ID: UBTU-20-010432
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.		●	●

4.2.1.2 Ensure rsyslog Service is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG - Server
- STIG - 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 one of the following commands to verify `rsyslog` is enabled:

```
# systemctl is-enabled rsyslog
```

Verify result is enabled.

Remediation:

Run the following commands to enable `rsyslog`:

```
# systemctl --now enable rsyslog
```

Additional Information:

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

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238353
Rule ID: SV-238353r654234_rule
STIG ID: UBTU-20-010432
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>		●	●

4.2.1.3 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:

```
*. emerg :omusrmsg:*
auth,authpriv.* /var/log/auth.log
mail.* -/var/log/mail
mail.info -/var/log/mail.info
mail.warning -/var/log/mail.warn
mail.err /var/log/mail.err
news.crit -/var/log/news/news.crit
news.err -/var/log/news/news.err
news.notice -/var/log/news/news.notice
*.=warning;*.=err -/var/log/warn
*.crit /var/log/warn
*.*=mail.none;news.none -/var/log/messages
local0,local1.* -/var/log/localmessages
local2,local3.* -/var/log/localmessages
local4,local5.* -/var/log/localmessages
local6,local7.* -/var/log/localmessages
```

Run the following command to reload the `rsyslog` configuration:

```
# systemctl reload 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.		●	●

4.2.1.4 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 every instance of \$FileCreateMode is 0640 or more restrictive:

```
# grep ^\s*\$FileCreateMode /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

If \$FileCreateMode is not found, the default value 0644 is used and at least one \$FileCreateMode has to be added.

Remediation:

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and set every instance of \$FileCreateMode to 0640 or more restrictive:

```
$FileCreateMode 0640
```

References:

1. See the rsyslog.conf(5) man page for more information.

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.	●	●	●

4.2.1.5 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

Note: Ensure that the selection of logfiles being sent follows local site policy

Audit:

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that logs are sent to a central host.

```
# grep -E '^\\s*([^\#]+\\s+)?action\\(((^#]+\\s+)?\\bttarget=\\"?[^"]+"?\\b' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include `target=<FQDN or IP of remote loghost>`

OR

```
# grep -E '^#[^\\s]*\\s*\\S+\\.\\*\\s+@' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include either the FQDN or the IP of the remote loghost

Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and add one of the following lines:

Newer syntax:

```
<files to sent to the remote log server> action(type="omfwd" target "<FQDN or  
ip of loghost>" port "<port number>" protocol="tcp"  
action.resumeRetryCount "<number of re-tries>"  
queue.type="LinkedList"  
queue.size=<number of messages to queue>")
```

Example:

```
*.* action(type="omfwd" target="192.168.2.100" port="514" protocol="tcp"  
action.resumeRetryCount="100"  
queue.type="LinkedList" queue.size="1000")
```

Older syntax:

```
*.* @@<FQDN or ip of loghost>
```

Example:

```
*.* @@192.168.2.100
```

Run the following command to reload the `rsyslog` 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

The `*.*` is a "wildcard" to send all logs to the remote loghost

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.</p>		●	●
v7	<p>6.6 Deploy SIEM or Log Analytic tool Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.</p>		●	●
v7	<p>6.8 Regularly Tune SIEM On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.</p>			●

4.2.1.6 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.

Note: The \$ModLoad imtcp line can have the .so extension added to the end of the module, or use the full path to the module

Audit:

Run the following commands: and verify the resulting lines are:

- Not commented on designated log hosts
- Commented or not present on all others

Run the following command and verify the output for \$ModLoad imtcp

```
# grep '$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output for designated log hosts:

```
$ModLoad imtcp
```

Output for systems that are not log hosts: (*No output is also acceptable*)

```
# $ModLoad imtcp
```

Run the following command and verify the output for '\$InputTCPServerRun'

```
# grep '$InputTCPServerRun' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output for designated log hosts:

```
$InputTCPServerRun 514
```

Output for systems that are not log hosts: (*No output is also acceptable*)

```
# $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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. 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.	●	●	●

4.2.1.7 Ensure remote access methods are monitored (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must monitor remote access methods

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 also 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 Ubuntu operating system monitors all remote access methods.

Check that remote access methods are being logged by running the following command:

```
# grep -E -r '^(auth,authpriv\.\.*|daemon\.\*)' /etc/rsyslog.*  
/etc/rsyslog.d/50-default.conf:auth,authpriv.* /var/log/auth.log  
/etc/rsyslog.d/50-default.conf:daemon.notice /var/log/messages
```

If "auth.", "authpriv.", or "daemon.*" are not configured to be logged in at least one of the config files, this is a finding.

Remediation:

Configure the Ubuntu operating system to monitor all remote access methods by adding the following lines to the "/etc/rsyslog.d/50-default.conf" file:

```
auth.*,authpriv.* /var/log/secure  
daemon.notice /var/log/messages
```

For the changes to take effect, restart the "rsyslog" service with the following command:

```
# systemctl restart rsyslog.service
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238324
Rule ID: SV-238324r654147_rule
STIG ID: UBTU-20-010403
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.	●	●	●

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 kmsg

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.

Notes:

- *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*

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 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>

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.

*Note: 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*

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 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>

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.

*Note: 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*

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 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>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.10 Retain Audit Logs Retain audit logs across enterprise assets for a minimum of 90 days.		●	●
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 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/rsyslog` is the configuration file used to rotate log files created by `rsyslog`.

Note: 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.

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/rsyslog` and verify logs are rotated according to site policy.

Remediation:

Edit `/etc/logrotate.conf` and `/etc/logrotate.d/rsyslog` to ensure logs are rotated according to site policy.

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.		●	●

4.2.4 Ensure logrotate assigns appropriate permissions (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Log files 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 command:

```
# grep -Es "^\s*create\s+\S+" /etc/logrotate.conf /etc/logrotate.d/* | grep -E -v "\s(0)?[0-6][04]0\s"
```

Nothing should be returned

Remediation:

Edit `/etc/logrotate.conf` and update the `create` line to read 0640 or more restrictive, following local site policy

Example:

```
create 0640 root utmp
```

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.	●	●	●

4.2.5 Ensure permissions on all logfiles are configured (Automated)

Profile Applicability:

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

Description:

Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well.

Note: You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.

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 other has no permissions on any files and group does not have write or execute permissions on any files:

```
# find /var/log -type f -ls
```

Remediation:

Run the following commands to set permissions on all existing log files:

```
find /var/log -type f -exec chmod g-wx,o-rwx "{}" + -o -type d -exec chmod g-w,o-rwx "{}" +
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238337
Rule ID: SV-238337r654186_rule
STIG ID: UBTU-20-010416
Severity: CAT II

Vul ID: V-238340
Rule ID: SV-238340r654195_rule
STIG ID: UBTU-20-010419
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.	●	●	●

4.2.6 Ensure /var/log is group-owned by syslog (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must configure the /var/log directory to be group-owned by syslog.

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 Ubuntu operating system configures the "/var/log" directory to be group-owned by syslog with the following command:

```
# stat -c "%n %G" /var/log  
/var/log syslog
```

If the "/var/log" directory is not group-owned by syslog, this is a finding.

Remediation:

Configure the Ubuntu operating system to have syslog group-own the "/var/log" directory by running the following command:

```
# chgrp syslog /var/log
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238338
Rule ID: SV-238338r654189_rule
STIG ID: UBTU-20-010417
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.	●	●	●

4.2.7 Ensure /var/log is owned by root (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must configure the /var/log directory to 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 Ubuntu operating system configures the "/var/log" directory to be owned by root with the following command:

```
# stat -c "%n %U" /var/log  
/var/log root
```

If the "/var/log" directory is not owned by root, this is a finding.

Remediation:

Configure the Ubuntu operating system to have root own the "/var/log" directory by running the following command:

```
# chown root /var/log
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238339
Rule ID: SV-238339r654192_rule
STIG ID: UBTU-20-010418
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.	●	●	●

4.2.8 Ensure /var/log/syslog is group-owned by adm (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must configure the /var/log/syslog file to be group-owned by adm.

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 Ubuntu operating system configures the "/var/log/syslog" file to be group-owned by adm with the following command:

```
# stat -c "%n %G" /var/log/syslog  
/var/log/syslog adm
```

If the "/var/log/syslog" file is not group-owned by adm, this is a finding.

Remediation:

Configure the Ubuntu operating system to have adm group-own the "/var/log/syslog" file by running the following command:

```
# chgrp adm /var/log/syslog
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238341
Rule ID: SV-238341r654198_rule
STIG ID: UBTU-20-010420
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.	●	●	●

4.2.9 Ensure /var/log/syslog is owned by syslog (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must configure /var/log/syslog file to be owned by syslog.

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 Ubuntu operating system configures the "/var/log/syslog" file to be owned by syslog with the following command:

```
# stat -c "%n %U" /var/log/syslog  
/var/log/syslog syslog
```

If the "/var/log/syslog" file is not owned by syslog, this is a finding.

Remediation:

Configure the Ubuntu operating system to have syslog own the "/var/log/syslog" file by running the following command:

```
# chown syslog /var/log/syslog
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238342
Rule ID: SV-238342r654201_rule
STIG ID: UBTU-20-010421
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.	●	●	●

4.2.10 Ensure /var/log/syslog is 0640 or more restrictive (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must configure /var/log/syslog file with 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 Ubuntu operating system configures the "/var/log/syslog" file with mode 0640 or less permissive by running the following command:

```
# stat -c "%n %a" /var/log/syslog  
/var/log/syslog 640
```

If a value of "640" or less permissive is not returned, this is a finding.

Remediation:

Configure the Ubuntu operating system to have permissions of 0640 for the "/var/log/syslog" file by running the following command:

```
# chmod 0640 /var/log/syslog
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238343
Rule ID: SV-238343r654204_rule
STIG ID: UBTU-20-010422
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.	●	●	●

5 Access, Authentication and Authorization

5.1 Configure time-based job schedulers

`cron` is a time-based job scheduler used to schedule jobs, commands or shell scripts, to run periodically at fixed times, dates, or intervals.

`at` provides the ability to execute a command or shell script at a specified date and hour, or after a given interval of time.

Notes:

- *Other methods exist for scheduling jobs, such as `systemd timers`. If another method is used, it should be secured in accordance with local site policy*
- *`systemd timers` are `systemd` unit files whose name ends in `.timer` that control `.service` files or events*
 - *Timers can be used as an alternative to `cron` and `at`*
 - *Timers have built-in support for calendar time events, monotonic time events, and can be run asynchronously*
- *If `cron` and `at` are not installed, this section can be skipped*

5.1.1 Ensure cron daemon is enabled and running (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `cron` daemon is used to execute batch jobs on the system.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

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 following command to verify `cron` is enabled:

```
# systemctl is-enabled cron  
enabled
```

Run the following command to verify that `cron` is running:

```
# systemctl status cron | grep 'Active: active (running) '  
Active: active (running) since <Day Date Time>
```

Remediation:

Run the following command to enable and start `cron`:

```
# systemctl --now enable cron
```

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.

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

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	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.	●	●	●

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.

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

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 the /etc/cron.hourly directory:

```
# 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	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.	●	●	●

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.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

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 the `/etc/cron.daily` directory:

```
# 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	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.	●	●	●

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.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

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 the /etc/cron.weekly directory:

```
# 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	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.	●	●	●

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.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

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 the /etc/cron.monthly directory:

```
# 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	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.	●	●	●

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.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

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 the `/etc/cron.d` directory:

```
# 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	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.	●	●	●

5.1.8 Ensure cron is restricted to authorized users (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure `/etc/cron.allow` to allow specific users to use this service. If `/etc/cron.allow` does not exist, then `/etc/cron.deny` is checked. Any user not specifically defined in this file is allowed to use cron. By removing the file, only users in `/etc/cron.allow` are allowed to use cron.

Notes:

- *Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy*
- *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 and verify that /etc/cron.deny does not exist:

```
# stat /etc/cron.deny  
stat: cannot stat `/etc/cron.deny': No such file or directory
```

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access`, does not grant write or execute to group, and does not grant permissions to other for /etc/cron.allow:

```
# stat /etc/cron.allow  
Access: (0640/-rw-r----)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to remove /etc/cron.deny:

```
# rm /etc/cron.deny
```

Run the following command to create /etc/cron.allow

```
# touch /etc/cron.allow
```

Run the following commands to set permissions and ownership for /etc/cron.allow:

```
# chmod g-wx,o-rwx /etc/cron.allow  
# chown root:root /etc/cron.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	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.	●	●	●

5.1.9 Ensure at is restricted to authorized users (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure /etc/at.allow to allow specific users to use this service. If /etc/at.allow does not exist, then /etc/at.deny is checked. Any user not specifically defined in this file is allowed to use at. By removing the file, only users in /etc/at.allow are allowed to use at.

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, at should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

On many systems, only the system administrator is authorized to schedule at jobs. Using the at.allow file to control who can run at 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 and verify that /etc/at.deny does not exist:

```
# stat /etc/at.deny
stat: cannot stat `/etc/at.deny': No such file or directory
```

Run the following command and verify Uid and Gid are both 0/root and Access, does not grant write or execute to group, and does not grant permissions to other for /etc/at.allow:

```
# stat /etc/at.allow
Access: (0640/-rw-r-----) Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to remove /etc/at.deny:

```
# rm /etc/at.deny
```

Run the following command to create /etc/at.allow

```
# touch /etc/at.allow
```

Run the following commands to set permissions and ownership for /etc/at.allow:

```
# chmod g-wx,o-rwx /etc/at.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	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.	●	●	●

5.2 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.

5.2.1 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.

Note: Use the sudo-ldap package if you need LDAP support for sudoers

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 and inspect the output to confirm that sudo is installed:

```
# dpkg -s sudo
```

OR

```
# dpkg -s sudo-ldap
```

Remediation:

Install sudo using the following command.

```
# apt install sudo
```

OR

```
# apt install sudo-ldap
```

References:

1. SUDO(8)
2. <http://www.sudo.ws/>

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	4.3 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.	●	●	●

5.2.2 Ensure sudo commands use pty (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Note: 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.

Rationale:

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

Audit:

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

Run the following command:

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

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)

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	4.3 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.	●	●	●

5.2.3 Ensure sudo log file exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo can use a custom log file.

Note: 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.

Rationale:

A sudo log file simplifies auditing of sudo commands

Audit:

Verify that sudo has a custom log file configured

Run the following command:

```
# grep -Ei '^Defaults\s+logfile=\S+' /etc/sudoers /etc/sudoers.d/*
```

Remediation:

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

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

Example:

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

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	6.3 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.		●	●

5.2.4 Ensure only users who need access to security functions are part of sudo group (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must ensure only users who need access to security functions are part of sudo group.

Rationale:

An isolation boundary provides access control and protects the integrity of the hardware, software, and firmware that perform security functions.

Security functions are 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. Operating systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk and address space protections that protect executing code.

Developers and implementers can increase the assurance in security functions by employing well-defined security policy models; structured, disciplined, and rigorous hardware and software development techniques; and sound system/security engineering principles. Implementation may include isolation of memory space and libraries.

The Ubuntu operating system restricts access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

Audit:

Verify the sudo group has only members who should have access to security functions.

```
# grep ^sudo: /etc/group  
sudo:x:27:foo
```

If the sudo group contains users not needing access to security functions, this is a finding.

Remediation:

Configure the sudo group with only members requiring access to security functions.

To remove a user from the sudo group, run:

```
# sudo gpasswd -d <username> sudo
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238206
Rule ID: SV-238206r653793_rule
STIG ID: UBTU-20-010012
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u></p> <p>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.</p>	●	●	●
v7	<p>4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u></p> <p>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>	●	●	●

5.2.5 Ensure users must reauthenticate for privilege escalation or when changing roles (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must require users to reauthenticate for privilege escalation or when changing roles.

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

Audit:

Verify the "/etc/sudoers" file has no occurrences of "NOPASSWD" or "!authenticate" by running the following command:

```
# grep -Ei '(nopasswd|!authenticate)' /etc/sudoers /etc/sudoers.d/*
```

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

Remediation:

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

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238208
Rule ID: SV-238208r653799_rule
STIG ID: UBTU-20-010014
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> 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 <u>Ensure the Use of Dedicated Administrative Accounts</u> 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.	●	●	●

5.3 Configure SSH Server

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.

`sshd` reads configuration data from `/etc/ssh/sshd_config` (or the file specified with `-f` on the command line). The file contains keyword-argument pairs, one per line. For each keyword, the first obtained value will be used. Lines starting with '#' and empty lines are interpreted as comments. Arguments may optionally be enclosed in double quotes ("") in order to represent arguments containing spaces.

Notes:

- The recommendations in this section are based on and tested against openSSH Server version 8.2p1. If another version of SSH Server is in use on the system, please confirm these settings with the vendors documentation
- 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.**
- `/etc/ssh/sshd_config.d/*.conf` files are included at the start of the configuration file, so options set there will override those in `/etc/ssh/sshd_config`.
- the Debian openssh-server package sets several options as standard in `/etc/ssh/sshd_config` which are not the default in `sshd(8)`:
 - `Include /etc/ssh/sshd_config.d/*.conf`
 - `ChallengeResponseAuthentication no`
 - `X11Forwarding yes`
 - `PrintMotd no`
 - `AcceptEnv LANG LC_*`
 - `Subsystem sftp /usr/lib/openssh/sftp-server`
 - `UsePAM yes`
- Once all configuration changes have been made to `/etc/ssh/sshd_config`, the `sshd` configuration must be reloaded.
- Run the following command to reload the `sshd` configuration:

```
# service sshd reload
```

5.3.1 Ensure SSH is installed and active (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must use SSH to protect the confidentiality and integrity of transmitted information.

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-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Verify the SSH package is installed with the following command:

```
# dpkg -l | grep openssh  
  
ii openssh-client 1:7.6p1-4ubuntu0.1 amd64 secure shell (SSH) client, for  
secure access to remote machines  
ii openssh-server 1:7.6p1-4ubuntu0.1 amd64 secure shell (SSH) server, for  
secure access from remote machines  
ii openssh-sftp-server 1:7.6p1-4ubuntu0.1 amd64 secure shell (SSH) sftp  
server module, for SFTP access from remote machines
```

If the "openssh" server package is not installed, this is a finding.

Verify the "sshd.service" is loaded and active with the following command:

```
# systemctl status sshd.service | egrep -i "(active|loaded)"  
  
Loaded: loaded (/lib/systemd/system/sshd.service; enabled; vendor preset:  
enabled)  
Active: active (running) since Thu 2019-01-24 22:52:58 UTC; 1 weeks 3 days  
ago
```

If "sshd.service" is not active or loaded, this is a finding.

Remediation:

Install the "ssh" meta-package on the system with the following command:

```
# apt install ssh
```

Enable the "ssh" service to start automatically on reboot with the following command:

```
# systemctl enable sshd.service
```

ensure the "ssh" service is running

```
# systemctl start sshd.service
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238215
Rule ID: SV-238215r653820_rule
STIG ID: UBTU-20-010042
Severity: CAT I

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.		●	●

5.3.2 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
```

Default Value:

Access: (0600/-rw-----) 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	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.	●	●	●

5.3.3 Ensure permissions on SSH private host key files are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify 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: 1675          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 794321     Links: 1
Access: (0600/-rw-----) Uid: ( 0/    root)  Gid: ( 0/    root)
Access: 2021-03-01 06:25:08.633246149 -0800
Modify: 2021-01-29 06:42:16.001324236 -0800
Change: 2021-01-29 06:42:16.001324236 -0800
 Birth: -
File: '/etc/ssh/ssh_host_ecdsa_key'
  Size: 227           Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 794325     Links: 1
Access: (0600/-rw-----) Uid: ( 0/    root)  Gid: ( 0/    root)
Access: 2021-03-01 06:25:08.633246149 -0800
Modify: 2021-01-29 06:42:16.173327263 -0800
Change: 2021-01-29 06:42:16.173327263 -0800
 Birth: -
File: '/etc/ssh/ssh_host_ed25519_key'
  Size: 399           Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 794327     Links: 1
Access: (0600/-rw-----) Uid: ( 0/    root)  Gid: ( 0/    root)
Access: 2021-03-01 06:25:08.633246149 -0800
Modify: 2021-01-29 06:42:16.185327474 -0800
Change: 2021-01-29 06:42:16.185327474 -0800
 Birth: -
File: '/etc/ssh/ssh_host_dsa_key'
  Size: 672           Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 794323     Links: 1
Access: (0600/-rw-----) Uid: ( 0/    root)  Gid: ( 0/    root)
Access: 2021-03-01 06:25:08.645246255 -0800
Modify: 2021-01-29 06:42:16.161327052 -0800
Change: 2021-01-29 06:42:16.161327052 -0800
 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 chown root:root {} \;
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chmod u-x,go-rwx {} \;
```

Default Value:

Access: (0600/-rw-----) Uid: (0/ root) Gid: (0/ root)

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>	●	●	●

5.3.4 Ensure permissions on SSH public host key files are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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)

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.	●	●	●

5.3.5 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 command:

```
sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -Ei '^\\s*(allow|deny) (users|groups) \\s+\\S+'
```

Verify that the output matches at least one of the following lines:

```
allowusers <userlist>
allowgroups <grouplist>
denyusers <userlist>
denygroups <grouplist>
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` 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.	●	●	●

5.3.6 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 -is 'loglevel' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf | grep -Evi '(VERBOSE|INFO)'
```

```
Nothing should be returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` 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.		●	●

5.3.7 Ensure SSH X11 forwarding is disabled (Automated)

Profile Applicability:

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

Description:

The X11Forwarding parameter provides the ability to tunnel X11 traffic through an existing SSH shell session 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.

Impact:

X11 programs on the server will not be able to be forwarded to a ssh-client display.

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 -Eis '^s*x11forwarding\s+yes' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
Nothing is returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` to set the parameter as follows:

```
X11Forwarding no
```

Default Value:

`X11Forwarding yes`

References:

1. `SSHD_CONFIG(5)`

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238219
Rule ID: SV-238219r653832_rule
STIG ID: UBTU-20-010048
Severity: CAT I

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.	●		●

5.3.8 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 -Eis '^s*maxauthtries\s+([5-9] | [1-9][0-9]+)' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
  
Nothing is returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` 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	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	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

5.3.9 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 -Eis '^s*ignorerhosts\s+no\b' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
  
Nothing should be returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` 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	<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>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.</p>		●	●

5.3.10 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.

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 -Eis '^s*HostbasedAuthentication\s+yes' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
  
Nothing should be returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` to set the `HostbasedAuthentication` 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.		●	●

5.3.11 Ensure SSH root login is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PermitRootLogin` parameter specifies if the root user can log in using ssh.

Rationale:

Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via `sudo`. 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 -Eis '^s*PermitRootLogin\s+yes' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
  
Nothing should be returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` to set the `PermitRootLogin` parameter as follows:

```
PermitRootLogin no
```

Default Value:

`PermitRootLogin without-password`

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	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.	●	●	●

5.3.12 Ensure SSH PermitEmptyPasswords is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG - Server
- STIG - 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 -Eis '^s*PermitEmptyPasswords\s+yes' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
  
Nothing should be returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` to set the `PermitEmptyPasswords` parameter as follows:

```
PermitEmptyPasswords no
```

Default Value:

PermitEmptyPasswords no

References:

1. SSHD_CONFIG(5)

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238218
Rule ID: SV-238218r653829_rule
STIG ID: UBTU-20-010047
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.		●	●

5.3.13 Ensure SSH PermitUserEnvironment is disabled (Automated)

Profile Applicability:

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

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 a Trojan's 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 -Eis '^s*PermitUserEnvironment\s+yes' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
  
Nothing should be returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` to set the parameter as follows:

```
PermitUserEnvironment no
```

Default Value:

PermitUserEnvironment no

References:

1. SSHD_CONFIG(5)

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238218
Rule ID: SV-238218r653829_rule
STIG ID: UBTU-20-010047
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.	●	●	●

5.3.14 Ensure only strong Ciphers are used (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This variable limits the ciphers that SSH can use during communication.

Note: Some organizations may have stricter requirements for approved ciphers. Ensure that ciphers used are in compliance with site policy.

Rationale:

Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised.

- The DES, Triple DES, and Blowfish ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack
- The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue
- The passwords used during an SSH session encrypted with RC4 can be recovered by an attacker who is able to capture and replay the session
- Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors

Audit:

Run the following command and verify the output:

```
# sshd -T -C user=root -C host="$ (hostname)" -C addr="$ (grep $ (hostname) /etc/hosts | awk '{print $1}')" | grep -Ei '^s*ciphers\s+([^\#]+,)?(3des-cbc|aes128-cbc|aes192-cbc|aes256-cbc|arcfour|arcfour128|arcfour256|blowfish-cbc|cast128-cbc|rijndael-cbc@lysator.liu.se)\b'
```

Nothing should be returned

Run the following command and verify the output:

```
grep -Eis '^s*ciphers\s+([^\#]+,)?(3des-cbc|aes128-cbc|aes192-cbc|aes256-cbc|arcfour|arcfour128|arcfour256|blowfish-cbc|cast128-cbc|rijndael-cbc@lysator.liu.se)\b' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf
```

Nothing should be returned

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` and add or modify the `Ciphers` line to contain a comma separated list of the site approved ciphers
Example:

```
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
```

Default Value:

Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

References:

1. <https://nvd.nist.gov/vuln/detail/CVE-2016-2183>
2. <https://nvd.nist.gov/vuln/detail/CVE-2015-2808>
3. <https://www.kb.cert.org/vuls/id/565052>
4. <https://www.openssh.com/txt/cbc.adv>
5. <https://nvd.nist.gov/vuln/detail/CVE-2008-5161>
6. <https://nvd.nist.gov/vuln/detail/CVE-2013-4548>
7. <https://www.kb.cert.org/vuls/id/565052>
8. <https://www.openssh.com/txt/cbc.adv>
9. SSHD_CONFIG(5)

Additional Information:

Weak Ciphers:

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Ciphers supported by openSSH v8.2p1:

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

Currently FIPS 140-2 approved ciphers:

```
aes256-gcm@openssh.com
aes128-gcm@openssh.com
aes256-ctr
aes192-ctr
aes128-ctr
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>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).</p>		●	●
v7	<p>14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.</p>		●	●

5.3.15 Ensure only FIPS 140-2 approved Ciphers are used (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must configure the SSH daemon to use FIPS 140-2 approved ciphers to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.

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.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network.

Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes.

By specifying a cipher list with the order of ciphers being in a "strongest to weakest" orientation, the system will automatically attempt to use the strongest cipher for securing SSH connections.

Satisfies: SRG-OS-000424-GPOS-00188, SRG-OS-000033-GPOS-00014, SRG-OS-000394-GPOS-00174

Audit:

Verify the SSH daemon is configured to only implement FIPS-approved algorithms by running the following command:

```
# grep -E 'Ciphers' /etc/ssh/sshd_config  
Ciphers aes256-ctr,aes192-ctr, aes128-ctr
```

If any ciphers other than "aes256-ctr", "aes192-ctr", or "aes128-ctr" are listed, the order differs from the example above, the "Ciphers" keyword is missing, or the returned line is commented out, this is a finding.

Remediation:

Configure the Ubuntu operating system to allow the SSH daemon to only implement FIPS-approved algorithms.

Add the following line (or modify the line to have the required value) to the "/etc/ssh/sshd_config" file (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):

```
Ciphers aes256-ctr,aes192-ctr, aes128-ctr
```

Restart the SSH daemon for the changes to take effect:

```
# systemctl restart sshd.service
```

Default Value:

Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238217
Rule ID: SV-238217r653826_rule
STIG ID: UBTU-20-010044
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.		●	●

5.3.16 Ensure only strong MAC algorithms are used (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This variable Specifies the available MAC (message authentication code) algorithms. The MAC algorithm is used in protocol version 2 for data integrity protection. Multiple algorithms must be comma-separated.

Note: Some organizations may have stricter requirements for approved MACs. Ensure that MACs used are in compliance with site policy.

Rationale:

MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information

Audit:

Run the following command and verify the output:

```
# sshd -T -C user=root -C host="$ (hostname)" -C addr="$ (grep $ (hostname) /etc/hosts | awk '{print $1}')" | grep -Ei '^s*macs\s+([^\#]+,)?(hmac-md5|hmac-md5-96|hmac-ripemd160|hmac-sha1|hmac-sha1-96|umac-64@openssh\.com|hmac-md5-etm@openssh\.com|hmac-md5-96-etm@openssh\.com|hmac-ripemd160-etm@openssh\.com|hmac-sha1-etm@openssh\.com|hmac-sha1-96-etm@openssh\.com|umac-64-etm@openssh\.com|umac-128-etm@openssh\.com)\b'
```

Nothing should be returned

Run the following command and verify the output:

```
# grep -Eis '^s*macs\s+([^\#]+,)?(hmac-md5|hmac-md5-96|hmac-ripemd160|hmac-sha1|hmac-sha1-96|umac-64@openssh\.com|hmac-md5-etm@openssh\.com|hmac-md5-96-etm@openssh\.com|hmac-ripemd160-etm@openssh\.com|hmac-sha1-etm@openssh\.com|hmac-sha1-96-etm@openssh\.com|umac-64-etm@openssh\.com|umac-128-etm@openssh\.com)\b' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf
```

Nothing should be returned

Remediation:

Edit /etc/ssh/sshd_config or a file in /ssh/sshd_config.d/ ending in .conf and add or modify the MACs line to contain a comma separated list of the site approved MACs

Example:

```
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256
```

Default Value:

MACs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

References:

1. More information on SSH downgrade attacks can be found here:
<http://www.mitls.org/pages/attacks/SLOTH>
2. SSHD_CONFIG(5)

Additional Information:

Weak MAC algorithms:

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-sha1
hmac-sha1-96
umac-64@openssh.com
umac-128@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
```

MAC algorithms supported by openSSH v8.2p1:

```
hmac-md5
hmac-md5-96
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-512
umac-64@openssh.com
umac-128@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
```

"strong" MAC algorithms currently FIPS 140-2 approved:

```
hmac-sha2-512-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-
256, hmac-sha2-512
```

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.		●	●

5.3.17 Ensure only FIPS 140-2 approved MAC algorithms are used (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The Ubuntu operating system must configure the SSH daemon to use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hashes to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.

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. Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network.

Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes.

Satisfies: SRG-OS-000424-GPOS-00188, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173

Audit:

Verify the SSH daemon is configured to only use MACs that employ FIPS 140-2 approved ciphers with the following command:

```
# grep -i macs /etc/ssh/sshd_config  
MACs hmac-sha2-512,hmac-sha2-256
```

If any ciphers other than "hmac-sha2-512" or "hmac-sha2-256" are listed, the order differs from the example above, or the returned line is commented out, this is a finding.

Remediation:

Configure the Ubuntu operating system to allow the SSH daemon to only use MACs that employ FIPS 140-2 approved ciphers.

Add the following line (or modify the line to have the required value) to the "/etc/ssh/sshd_config" file (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):

```
MACs hmac-sha2-512,hmac-sha2-256
```

Restart the SSH daemon for the changes to take effect:

```
# systemctl reload sshd.service
```

Default Value:

MACs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

References:

1. [SSHD_CONFIG\(5\)](#)

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238216
Rule ID: SV-238216r654316_rule
STIG ID: UBTU-20-010043
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.		●	●

5.3.18 Ensure only strong Key Exchange algorithms are used (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received

Note: Some organizations may have stricter requirements for approved Key Exchange algorithms. Ensure that Key Exchange algorithms used are in compliance with site policy.

Rationale:

Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

Audit:

Run the following command and verify the output:

```
# sshd -T -C user=root -C host="$ (hostname)" -C addr="$ (grep $ (hostname) /etc/hosts | awk '{print $1}')" | grep -Ei '^\\s*kexalgorithms\\s+([^#]+,)?(diffie-hellman-group1-sha1|diffie-hellman-group14-sha1|diffie-hellman-group-exchange-sha1)\\b'
```

Nothing should be returned

Run the following command and verify the output:

```
# grep -Ei '^\\s*kexalgorithms\\s+([^#]+,)?(diffie-hellman-group1-sha1|diffie-hellman-group14-sha1|diffie-hellman-group-exchange-sha1)\\b' /etc/ssh/sshd_config
```

Nothing should be returned

Remediation:

Edit /etc/ssh/sshd_config or a file in /ssh/sshd_config.d/ ending in .conf and add or modify the KexAlgorithms line to contain a comma separated list of the site approved key exchange algorithms.

Example:

```
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
```

Default Value:

```
kexalgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256
```

References:

1. SSHD_CONFIG(5)

Additional Information:

Weak Key Exchange Algorithms:

```
diffie-hellman-group1-sha1  
diffie-hellman-group14-sha1  
diffie-hellman-group-exchange-sha1
```

Key Exchange algorithms supported by OpenSSH 8.2p1:

```
curve25519-sha256  
curve25519-sha256@libssh.org  
diffie-hellman-group1-sha1  
diffie-hellman-group14-sha1  
diffie-hellman-group14-sha256  
diffie-hellman-group16-sha512  
diffie-hellman-group18-sha512  
diffie-hellman-group-exchange-sha1  
diffie-hellman-group-exchange-sha256  
ecdh-sha2-nistp256  
ecdh-sha2-nistp384  
ecdh-sha2-nistp521  
sntrup4591761x25519-sha512@tinyssh.org
```

"strong" Key Exchange Algorithms currently FIPS 140-2 approved:

```
ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-  
group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-  
sha512, diffie-hellman-group14-sha256
```

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.		●	●

5.3.19 Ensure SSH Idle Timeout Interval is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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: If the `ClientAliveInterval` is set to 15 seconds and the `ClientAliveCountMax` is set to 3, the client ssh session will be terminated after 45 seconds of idle time.

Rationale:

Having no timeout value associated with a connection could allow an ssh session to remain active after the connection with the client has been interrupted. Setting a timeout value reduces this risk.

- The recommended `ClientAliveInterval` setting is 300 seconds (5 minutes)
- The recommended `ClientAliveCountMax` setting is 3
- The ssh session would send three keep alive messages at 5 minute intervals. If no response is received after the third keep alive message, the ssh session would be terminated after 15 minutes.

Audit:

Run the following commands and verify ClientAliveInterval is between 1 and 300:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep clientaliveinterval  
clientaliveinterval 300
```

Run the following command and verify ClientAliveCountMax is between 1 and 3:

```
# 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 -Eis '^s*clientaliveinterval\s+(0|3[0-9][1-9]|4-9)[0-9][0-9]|1-9][0-9][0-9]+|[6-9]m|[1-9][0-9]+m)\b' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
  
Nothing should be returned  
  
# grep -Eis '^s*ClientAliveCountMax\s+(0|[4-9]|[1-9][0-9]+)\b' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf  
  
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 300 and ClientAliveCountMax between 1 and 3:

```
ClientAliveInterval 300  
ClientAliveCountMax 3
```

Default Value:

ClientAliveInterval 0

ClientAliveCountMax 3

References:

1. https://man.openbsd.org/sshd_config

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.	●	●	●

5.3.20 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 -Eis '^s*LoginGraceTime\s+(0|6[1-9]|7-9)[0-9]|1-9][0-9][0-9]+|^1m' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf  
Nothing should be returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` to set the parameter as follows:

```
LoginGraceTime 60
```

Default Value:

`LoginGraceTime 2m`

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.	●	●	●

5.3.21 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
```

Run the following command and verify that the output:

```
# grep -Eis '^s*Banner\s+?"none\b' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
  
Nothing is returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` to set the `Banner` parameter as follows:

```
Banner /etc/issue.net
```

Default Value:

Banner none

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.	●	●	●

5.3.22 Ensure SSH PAM is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG - Server
- STIG - 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(5) 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 -Eis '^s*UsePAM\s+no' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
  
Nothing should be returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` to set the parameter as follows:

```
usePAM yes
```

Default Value:

`usePAM yes`

References:

1. [SSHD_CONFIG\(5\)](#)

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238211
Rule ID: SV-238211r653808_rule
STIG ID: UBTU-20-010035
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.	●	●	●

5.3.23 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 -Eis '^s*AllowTcpForwarding\s+yes\b' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
  
Nothing should be returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` to set the parameter as follows:

```
AllowTcpForwarding no
```

Default Value:

AllowTcpForwarding yes

References:

1. <https://www.ssh.com/ssh/tunneling/example>
2. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></p> <p>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>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>	●	●	●
v7	<p>13.5 <u>Monitor and Detect Any Unauthorized Use of Encryption</u></p> <p>Monitor all traffic leaving the organization and detect any unauthorized use of encryption.</p>	●	●	●

5.3.24 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 -Eis '^s*maxstartups\s+(((1[1-9]|1-9)[0-9][0-9]+):([0-9]+):([0-9]+))|(([0-9]+):(3[1-9]|4-9)[0-9]|1-9)[0-9][0-9]+):([0-9]+))|(([0-9]+):(6[1-9]|7-9)[0-9]|1-9)[0-9][0-9]+))' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
  
Nothing should be returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` to set the `MaxStartups` 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.	●	●	●

5.3.25 Ensure SSH MaxSessions is limited (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxSessions` parameter Specifies the maximum number of open sessions permitted per network 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 -Eis '^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 /etc/ssh/sshd_config.d/*.conf  
Nothing should be returned
```

Remediation:

Edit `/etc/ssh/sshd_config` or a file in `/ssh/sshd_config.d/` ending in `.conf` 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.	●	●	●

5.3.26 Ensure network connections associated with SSH traffic are terminated after a period of inactivity (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must immediately terminate all network connections associated with SSH traffic after a period of inactivity.

Rationale:

Automatic session termination addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions.

Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on information system use.

This capability is typically reserved for specific Ubuntu operating system functionality where the system owner, data owner, or organization requires additional assurance.

Audit:

Verify that all network connections associated with SSH traffic automatically terminate after a period of inactivity.

Verify the "ClientAliveCountMax" variable is set in the "/etc/ssh/sshd_config" file by performing the following command:

```
# grep -i clientalivecountmax /etc/ssh/sshd_config  
ClientAliveCountMax 1
```

If "ClientAliveCountMax" is not set, is not set to "1", or is commented out, this is a finding.

Remediation:

Configure the Ubuntu operating system to automatically terminate inactive SSH sessions after a period of inactivity.

Modify or append the following line in the "/etc/ssh/sshd_config" file, replacing "[Count]" with a value of 1:

```
ClientAliveCountMax 1
```

Restart the SSH daemon for the changes to take effect:

```
# systemctl restart sshd.service
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238212
Rule ID: SV-238212r653811_rule
STIG ID: UBTU-20-010036
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.	●	●	●

*5.3.27 Ensure network connections associated with SSH traffic are terminated at the end of the session or 10 minutes of inactivity
(Automated)*

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The Ubuntu operating system must immediately terminate all network connections associated with SSH traffic at the end of the session or after 10 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 that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Audit:

Verify that all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity.

Verify 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
```

If "ClientAliveInterval" does not exist, is not set to a value of "600" or less in "/etc/ssh/sshd_config", or is commented out, this is a finding.

Remediation:

Configure the Ubuntu operating system to automatically terminate all network connections associated with SSH traffic at the end of a session or after a 10-minute period of inactivity. Modify or append the following line in the "/etc/ssh/sshd_config" file replacing "[Interval]" with a value of "600" or less:

```
ClientAliveInterval 600
```

Restart the SSH daemon for the changes to take effect:

```
# systemctl restart sshd.service
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238213
Rule ID: SV-238213r653814_rule
STIG ID: UBTU-20-010037
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.1 Establish and Maintain a Vulnerability Management Process Establish and maintain a documented vulnerability management process for enterprise assets. 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.	●	●	●

5.3.28 Ensure Standard Mandatory DoD Notice and Consent Banner displayed before granting any local or remote connection to the system (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting any local or remote connection to the system.

Rationale:

Display of a standardized and approved use notification before granting access to the publicly accessible 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."

Satisfies: SRG-OS-000228-GPOS-00088, SRG-OS-000023-GPOS-00006

Audit:

Verify the Ubuntu operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the Ubuntu operating system via an SSH logon with the following command:

```
# grep -i banner /etc/ssh/sshd_config  
Banner /etc/issue.net
```

The command will return the banner option along with the name of the file that contains the SSH banner. If the line is commented out, this is a finding.

Verify the specified banner file matches the Standard Mandatory DoD Notice and Consent Banner exactly:

```
# cat /etc/issue.net  
  
"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:

Set the parameter Banner in "/etc/ssh/sshd_config" to point to the "/etc/issue.net" file:

```
# sed -i '/^Banner/d' /etc/ssh/sshd_config  
# sed -i '$aBanner /etc/issue.net' /etc/ssh/sshd_config
```

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."
```

Restart the SSH daemon for the changes to take effect and then signal the SSH server to reload the configuration file:

```
# systemctl -s SIGHUP kill sshd
```

Additional Information:

```
Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 1 Benchmark Date: 10 Mar 2021
```

```
Vul ID: V-238214  
Rule ID: SV-238214r653817_rule  
STIG ID: UBTU-20-010038  
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.	●	●	●

5.3.29 Ensure X11UseLocalhost is enabled (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system 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 DISPLAY 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
```

Restart the SSH daemon for the changes to take effect:

```
# systemctl restart sshd.service
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238220
Rule ID: SV-238220r653835_rule
STIG ID: UBTU-20-010049
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.	●	●	●

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.

The following options are set in the `/etc/security/pwquality.conf` file:

- Password Length:
 - `minlen = 14` - password must be 14 characters or more
- Password complexity:
 - `minclass = 4` - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)
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 following is set in the `/etc/pam.d/common-password` file:

- `retry=3` - Allow 3 tries before sending back a failure. 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 to verify the minimum password length is 14 or more characters.

```
# grep '^s*minlen\s*' /etc/security/pwquality.conf  
minlen = 14
```

Run one of the following commands to verify the required password complexity:

```
# grep '^s*minclass\s*' /etc/security/pwquality.conf  
minclass = 4
```

OR

```
# grep -E '^s*[duol]credit\s*' /etc/security/pwquality.conf  
dcredit = -1  
ucredit = -1  
lcredit = -1  
ocredit = -1
```

Run the following command to verify the number of attempts allowed before sending back a failure are no more than 3

```
# grep -E  
'^s*password\s+(requisite|required)\s+pam_pwquality\.so\s+(\S+\s+)*retry=[1-  
3]\s*(\s+\S+\s*)*(\s+\#.* )?\$' /etc/pam.d/common-password  
  
password      requisite          pam_pwquality.so retry=3
```

Remediation:

Run the following command to install the pam_pwquality module:

```
apt install libpam-pwquality
```

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  
lccredit = -1
```

Edit the /etc/pam.d/common-password file to include the appropriate options for pam_pwquality.so and to conform to site policy:

```
password requisite pam_pwquality.so retry=3
```

Additional Information:

Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.

Settings in /etc/security/pwquality.conf must use spaces around the = symbol.

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 new and changed passwords use pwquality (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must be configured so that when passwords are changed or new passwords are established, pwquality must 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. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

Audit:

Verify the Ubuntu operating system has the "libpam-pwquality" package installed by running the following command:

```
# dpkg -l libpam-pwquality  
ii libpam-pwquality:amd64 1.4.0-2 amd64 PAM module to check password strength
```

If "libpam-pwquality" is not installed, this is a finding.

Verify that the operating system uses "pwquality" to enforce the password complexity rules.

Verify the pwquality module is being enforced by the Ubuntu operating system by running the following command:

```
# grep -i enforcing /etc/security/pwquality.conf  
enforcing = 1
```

If the value of "enforcing" is not "1" or the line is commented out, this is a finding.

Check for the use of "pwquality" with the following command:

```
# cat /etc/pam.d/common-password | grep requisite | grep pam_pwquality  
password requisite pam_pwquality.so retry=3
```

If no output is returned 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. Install the "pam_pwquality" package by using the following command:

```
# apt-get install libpam-pwquality -y
```

Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
enforcing = 1
```

Add the following line to "/etc/pam.d/common-password" (or modify the line to have the required value):

```
password requisite pam_pwquality.so retry=3
```

Note: The value of "retry" should be between "1" and "3".

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238228
Rule ID: SV-238228r653859 rule
STIG ID: UBTU-20-010057
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.		●	●

5.4.3 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. The first sets of changes are made to the PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM.

- deny= n - n represents the number of failed attempts before the account is locked
- unlock_time= n - n represents the number of seconds before the account is unlocked
- audit - Will log the user name into the system log if the user is not found.
- silent - Don't print informative messages. Set the lockout number and unlock time in accordance with 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` modules found in `/etc/pam.d/common-auth`:

```
# grep "pam_tally2" /etc/pam.d/common-auth
auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900
```

Verify the `pam_deny.so` module and `pam_tally2.so` modules are included in `/etc/pam.d/common-account`:

```
# grep -E "pam_(tally2|deny)\.so" /etc/pam.d/common-account
account requisite          pam_deny.so
account required           pam_tally2.so
```

Remediation:

Edit the /etc/pam.d/common-auth file and add the auth line below:

```
auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900
```

Edit the /etc/pam.d/common-account file and add the account lines bellow:

```
account requisite pam_deny.so  
account required pam_tally2.so
```

Additional Information:

- Add pam_tally2 to the account section `account required pam_tally2.so` for the counter to reset to 0 when using sudo
- 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.
- If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_tally2.so` module, the user can be unlocked by issuing the command `/sbin/pam_tally2 -u <username> --reset`. This command sets the failed count to 0, effectively unlocking the user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
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 password reuse is limited (Automated)

Profile Applicability:

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

Rationale:

Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password.

Audit:

Run the following commands and ensure the `remember` option is '5' or more and included in all results:

```
# grep -E
'^\s*password\s+required\s+pam_pwhistory\.so\s+([^\#]+\s+)?remember=([5-9]| [1-
9][0-9]+)\b' /etc/pam.d/common-password

password required pam_pwhistory.so remember=5
```

Remediation:

Edit the `/etc/pam.d/common-password` file to include the `remember` option and conform to site policy as shown:

```
password required pam_pwhistory.so remember=5
```

Additional Information:

Changes only apply to accounts configured on the local system.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238234
Rule ID: SV-238234r685225_rule
STIG ID: UBTU-20-010070
Severity: CAT III

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			

5.4.5 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:

Run the following commands and ensure the `sha512` option is included in all results:

```
# grep -E
'^\s*password\s+([\s+success=1\s+default=ignore\b|\s+required]\s+pam_unix\.so\s+([^\#]+\s+)?sha512\b' /etc/pam.d/common-password
```

Output should be similar to:

```
password      [success=1 default=ignore]      pam_unix.so obscure sha512
```

Remediation:

Edit the `/etc/pam.d/common-password` file to include the `sha512` option for `pam_unix.so` as shown:

```
password [success=1 default=ignore] pam_unix.so sha512
```

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

The following command can be used:

```
# awk -F: '($3 >= $(awk '/^s*UID_MIN/{print $2}' /etc/login.defs) && $1 != "nfsnobody") { print $1 }' /etc/passwd | xargs -n 1 chage -d 0
```

Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems

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	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

5.4.6 Ensure password is at least 15 characters (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must enforce a minimum 15-character password length.

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 exponentially increase the time and/or resources required to compromise the password.

Audit:

Verify the pwquality configuration file enforces a minimum 15-character password length by running the following command:

```
# grep -i ^minlen /etc/security/pwquality.conf  
minlen=15
```

If "minlen" parameter value is not "15" or higher or is commented out, this is a finding.

Remediation:

Configure the Ubuntu operating system to enforce a minimum 15-character password length.

Add or modify the "minlen" parameter value to the "/etc/security/pwquality.conf" file:

```
minlen=15
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238225
Rule ID: SV-238225r653850_rule
STIG ID: UBTU-20-010054
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.		●	●

5.4.7 Ensure password includes at least one upper-case character (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must enforce password complexity by requiring that at least one upper-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.

Audit:

Verify the Ubuntu operating system enforces password complexity by requiring that at least one upper-case character be used.

Determine if the field "ucredit" is set in the "/etc/security/pwquality.conf" file with the following command:

```
# grep -i "ucredit" /etc/security/pwquality.conf
ucredit=-1
```

If the "ucredit" parameter is greater than "-1" or is commented out, this is a finding.

Remediation:

Add or update the "/etc/security/pwquality.conf" file to contain the "ucredit" parameter:

```
ucredit=-1
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238221
Rule ID: SV-238221r653838_rule
STIG ID: UBTU-20-010050
Severity: CAT III

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.		●	●

5.4.8 Ensure password includes at least one lower-case character (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

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.

Audit:

Verify the Ubuntu operating system enforces password complexity by requiring that at least one lower-case character be used.

Determine if the field "lcredit" is set in the "/etc/security/pwquality.conf" file with the following command:

```
# grep -i "lcredit" /etc/security/pwquality.conf
lcredit=-1
```

If the "lcredit" parameter is greater than "-1" or is commented out, this is a finding.

Remediation:

Add or update the "/etc/security/pwquality.conf" file to contain the "lcredit" parameter:

```
lcredit=-1
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238222
Rule ID: SV-238222r653841_rule
STIG ID: UBTU-20-010051
Severity: CAT III

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.		●	●

5.4.9 Ensure password includes at least one numeric character (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

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.

Audit:

Verify the Ubuntu operating system enforces password complexity by requiring that at least one numeric character be used.

Determine if the field "dcredit" is set in the "/etc/security/pwquality.conf" file with the following command:

```
# grep -i "dcredit" /etc/security/pwquality.conf
dcredit=-1
```

If the "dcredit" parameter is greater than "-1" or is commented out, this is a finding.

Remediation:

Configure the Ubuntu operating system to enforce password complexity by requiring that at least one numeric character be used.

Add or update the "/etc/security/pwquality.conf" file to contain the "dcredit" parameter:

```
dcredit=-1
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238223
Rule ID: SV-238223r653844_rule
STIG ID: UBTU-20-010052
Severity: CAT III

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.		●	●

5.4.10 Ensure password includes at least one special character (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must enforce password complexity by requiring that at least one special 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 in determining 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.

Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ # \$ % ^ *.

Audit:

Determine if the field "ocredit" is set in the "/etc/security/pwquality.conf" file with the following command:

```
# grep -i "ocredit" /etc/security/pwquality.conf
ocredit=-1
```

If the "ocredit" parameter is greater than "-1" or is commented out, this is a finding.

Remediation:

Configure the Ubuntu operating system to enforce password complexity by requiring that at least one special character be used.

Add or update the following line in the "/etc/security/pwquality.conf" file to include the "ocredit=-1" parameter:

```
ocredit=-1
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238226
Rule ID: SV-238226r653853_rule
STIG ID: UBTU-20-010055
Severity: CAT III

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.		●	●

5.4.11 Ensure passwords can not use dictionary words (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must prevent the use of dictionary words for passwords.

Rationale:

If the Ubuntu operating system allows the user to select passwords based on dictionary words, then this increases the chances of password compromise by increasing the opportunity for successful guesses and brute-force attacks.

Audit:

Verify the Ubuntu operating system uses the "cracklib" library to prevent the use of dictionary words with the following command:

```
# grep dictcheck /etc/security/pwquality.conf  
dictcheck=1
```

If the "dictcheck" parameter is not set to "1" or is commented out, this is a finding.

Remediation:

Configure the Ubuntu operating system to prevent the use of dictionary words for passwords.

Add or update the following line in the "/etc/security/pwquality.conf" file to include the "dictcheck=1" parameter:

```
dictcheck=1
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238227
Rule ID: SV-238227r653856_rule
STIG ID: UBTU-20-010056
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.		●	●

5.4.12 Ensure change of at least 8 characters when passwords are changed (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must require the change of at least 8 characters when passwords are changed.

Rationale:

If the operating system allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. In other words, characters may be the same within the two passwords; however, the positions of the like characters must be different.

If the password length is an odd number then number of changed characters must be rounded up. For example, a password length of 15 characters must require the change of at least 8 characters.

Audit:

Verify the Ubuntu operating system requires the change of at least eight characters when passwords are changed.

Determine if the field "difok" is set in the "/etc/security/pwquality.conf" file with the following command:

```
# grep -i "difok" /etc/security/pwquality.conf  
difok=8
```

If the "difok" parameter is less than "8" or is commented out, this is a finding.

Remediation:

Configure the Ubuntu operating system to require the change of at least eight characters when passwords are changed.

Add or update the "/etc/security/pwquality.conf" file to include the "difok=8" parameter:

```
difok=8
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238224

Rule ID: SV-238224r653847_rule

STIG ID: UBTU-20-010053

Severity: CAT III

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.		●	●

5.4.13 Ensure lockout for failed password attempts until the locked account is released (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The Ubuntu operating system must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts have been made.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Audit:

Verify the Ubuntu operating system locks an account after three unsuccessful login attempts with following command:

```
# grep pam_tally2 /etc/pam.d/common-auth  
auth required pam_tally2.so onerr=fail deny=3
```

If no line is returned or the line is commented out, this is a finding.

If the line is missing "onerr=fail", this is a finding.

If the line has "deny" set to a value more than "3", this is a finding.

Remediation:

Configure the Ubuntu operating system to lock an account after three unsuccessful login attempts.

Edit the "/etc/pam.d/common-auth" file. The "pam_tally2.so" entry must be placed at the top of the "auth" stack.

Add the following line before the first "auth" entry in the file:

```
auth required pam_tally2.so onerr=fail deny=3
```

Additional Information:

- Add pam_tally2 to the account section `account required pam_tally2.so` for the counter to reset to 0 when using sudo
- 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.
- If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_tally2.so` module, the user can be unlocked by issuing the command `/sbin/pam_tally2 -u <username> --reset`. This command sets the failed count to 0, effectively unlocking the user.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238235
Rule ID: SV-238235r653880_rule
STIG ID: UBTU-20-010072
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
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.	●	●	●

5.4.14 Ensure the libpam-pkcs11 package is installed (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must implement multifactor authentication for remote access to privileged accounts in such a way that one of the factors is provided by a device separate from the system gaining access.

Rationale:

Using an authentication device, such as a 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 Common Access Card.

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 Ubuntu operating system has the packages required for multifactor authentication installed with the following commands:

```
# dpkg -l | grep libpam-pkcs11  
ii libpam-pkcs11 0.6.8-4 amd64 Fully featured PAM module for using PKCS#11  
smart cards
```

If the "libpam-pkcs11" package is not installed, this is a finding.

Remediation:

Configure the Ubuntu operating system to implement multifactor authentication by installing the required packages.

Install the "libpam-pkcs11" package on the system with the following command:

```
# apt install libpam-pkcs11
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238230
Rule ID: SV-238230r653865_rule
STIG ID: UBTU-20-010063
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
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.		●	●

5.4.15 Ensure the opensc-pkcs11 is installed (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

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.

DoD has mandated the use of the 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 Ubuntu operating system accepts PIV credentials.

Verify the "opensc-pkcs11" package is installed on the system with the following command:

```
# dpkg -l | grep opensc-pkcs11  
ii opensc-pkcs11:amd64 0.15.0-1Ubuntu1 amd64 Smart card utilities with  
support for PKCS#15 compatible cards
```

If the "opensc-pkcs11" package is not installed, this is a finding.

Remediation:

Configure the Ubuntu operating system to accept PIV credentials.

Install the "opensc-pkcs11" package using the following command:

```
# apt-get install opensc-pkcs11
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238231
Rule ID: SV-238231r653868_rule
STIG ID: UBTU-20-010064
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
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.		●	●

5.4.16 Ensure authenticated identity is mapped to the user or group account for PKI-based authentication (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

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.

Audit:

Verify that "use_mappers" is set to "pwent" in "/etc/pam_pkcs11/pam_pkcs11.conf" file:

```
# grep ^use_mappers /etc/pam_pkcs11/pam_pkcs11.conf  
use_mappers = pwent
```

If "use_mappers" is not found or the list does not contain "pwent" this is a finding.

Remediation:

Set "use_mappers=pwent" in "/etc/pam_pkcs11/pam_pkcs11.conf" or, if there is already a comma-separated list of mappers, add it to the list, separated by comma, and before the null mapper.

If the system is missing an "/etc/pam_pkcs11/" directory and an "/etc/pam_pkcs11/pam_pkcs11.conf", find an example to copy into place and modify accordingly at "/usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz".

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238201
Rule ID: SV-238201r653778_rule
STIG ID: UBTU-20-010006
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
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.		●	●

5.4.17 Ensure smart card logins for multifactor authentication for local and network access (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must implement smart card logins for multifactor authentication for local and network access to privileged and non-privileged accounts.

Rationale:

Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased.

Multifactor authentication requires using two or more factors to achieve authentication.

Factors include:

1. something a user knows (e.g., password/PIN);
2. something a user has (e.g., cryptographic identification device, token); and
3. something a user is (e.g., biometric).

A privileged account is defined as an information system account with authorizations of a privileged user.

Network access is defined as access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the internet).

The DoD CAC with DoD-approved PKI is an example of multifactor authentication.

Satisfies: SRG-OS-000105-GPOS-00052, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055

Audit:

Verify the Ubuntu operating system has the packages required for multifactor authentication installed with the following commands:

```
# dpkg -l | grep libpam-pkcs11  
ii libpam-pkcs11 0.6.8-4 amd64 Fully featured PAM module for using PKCS#11  
smart cards
```

If the "libpam-pkcs11" package is not installed, this is a finding.

Verify the sshd daemon allows public key authentication with the following,

```
# grep ^Pubkeyauthentication /etc/ssh/sshd_config  
PubkeyAuthentication yes
```

If this option is set to "no" or is missing, this is a finding.

Remediation:

Configure the Ubuntu operating system to use multifactor authentication for network access to accounts.

Add or update "pam_pkcs11.so" in "/etc/pam.d/common-auth" to match the following line:

```
auth [success=2 default=ignore] pam_pkcs11.so
```

Set the sshd option "PubkeyAuthentication yes" in the "/etc/ssh/sshd_config" file.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238210
Rule ID: SV-238210r653805_rule
STIG ID: UBTU-20-010033
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 <u>Require MFA for Remote Network Access</u> Require MFA for remote network access.	●	●	●
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

5.4.18 Ensure certificates are validated by constructing a certification path to an accepted trust anchor (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The Ubuntu operating system, for PKI-based authentication, must validate certificates 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.

Audit:

Verify the Ubuntu operating system, for PKI-based authentication, has valid certificates by constructing a certification path to an accepted trust anchor.

Determine which pkcs11 module is being used via the "use_pkcs11_module" in "/etc/pam_pkcs11/pam_pkcs11.conf" and then ensure "ca" is enabled in "cert_policy" with the following command:

```
# grep use_pkcs11_module /etc/pam_pkcs11/pam_pkcs11.conf | awk  
'/pkcs11_module opensc {/,/}/' /etc/pam_pkcs11/pam_pkcs11.conf | grep  
cert policy | grep ca  
  
cert_policy = ca,signature,ocsp_on;
```

If "cert_policy" is not set to "ca" or the line is commented out, this is a finding.

Remediation:

Configure the Ubuntu operating system, for PKI-based authentication, to validate certificates by constructing a certification path to an accepted trust anchor.

Determine which pkcs11 module is being used via the "use_pkcs11_module" in "/etc/pam_pkcs11/pam_pkcs11.conf" and ensure "ca" is enabled in "cert_policy".

Add or update the "cert_policy" to ensure "ca" is enabled:

```
cert_policy = ca,signature,ocsp_on;
```

If the system is missing an "/etc/pam_pkcs11/" directory and an "/etc/pam_pkcs11/pam_pkcs11.conf", find an example to copy into place and modify accordingly at "/usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz".

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238229
Rule ID: SV-238229r653862_rule
STIG ID: UBTU-20-010060
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 <u>Require MFA for Remote Network Access</u> Require MFA for remote network access.	●	●	●
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

5.4.19 Ensure Personal Identity Verification credentials are electronically verified (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must electronically verify Personal Identity Verification (PIV) credentials.

Rationale:

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DoD has mandated the use of the 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 Ubuntu operating system electronically verifies PIV credentials.

Verify that certificate status checking for multifactor authentication is implemented with the following command:

```
# sudo grep use_pkcs11_module /etc/pam_pkcs11/pam_pkcs11.conf | awk '/pkcs11_module opensc {/,/}/' /etc/pam_pkcs11/pam_pkcs11.conf | grep cert_policy | grep ocsp_on  
  
cert_policy = ca,signature,ocsp_on;
```

If "cert_policy" is not set to "ocsp_on", or the line is commented out, this is a finding.

Remediation:

Configure the Ubuntu operating system to do certificate status checking for multifactor authentication.

Modify all of the cert_policy lines in /etc/pam_pkcs11/pam_pkcs11.conf to include ocsp_on.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238232
Rule ID: SV-238232r653871_rule
STIG ID: UBTU-20-010065
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
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.		●	●

5.4.20 Ensure PKI local cache of revocation data (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system for PKI-based authentication, must implement a local cache of revocation data in case of the inability to access revocation information via the network.

Rationale:

Without configuring a local cache of revocation data, there is the potential to allow access to users who are no longer authorized (users with revoked certificates).

Audit:

Verify the Ubuntu operating system, for PKI-based authentication, uses local revocation data when unable to access it from the network.

Verify that "crl_offline" or "crl_auto" is part of the "cert_policy" definition in "/etc/pam_pkcs11/pam_pkcs11.conf" using the following command:

```
# grep cert_policy /etc/pam_pkcs11/pam_pkcs11.conf | grep -E --  
'crl_auto|crl_offline'  
  
cert_policy = ca,signature,ocsp_on,crl_auto;
```

If "cert_policy" is not set to include "crl_auto" or "crl_offline", this is a finding.

Remediation:

Configure the Ubuntu operating system, for PKI-based authentication, to use local revocation data when unable to access the network to obtain it remotely.

Add or update the "cert_policy" option in /etc/pam_pkcs11/pam_pkcs11.conf to include crl_auto or crl_offline.

```
cert_policy = ca,signature,ocsp_on, crl_auto;
```

If the system is missing an "/etc/pam_pkcs11/" directory and an "/etc/pam_pkcs11/pam_pkcs11.conf", find an example to copy into place and modify accordingly at "/usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz".

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238233
Rule ID: SV-238233r653874_rule
STIG ID: UBTU-20-010066
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
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.		●	●

5.4.21 Ensure logging delay after failed logon attempt (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must enforce a delay of at least 4 seconds between logon prompts following a failed logon attempt.

Rationale:

Limiting the number of logon attempts over a certain time interval reduces the chances that an unauthorized user may gain access to an account.

Audit:

Verify the operating system enforces a delay of at least 4 seconds between logon prompts following a failed logon attempt with the following command:

```
# grep pam_faiildelay /etc/pam.d/common-auth  
auth required pam_faiildelay.so delay=4000000
```

If the line is not present or is commented out, this is a finding.

Remediation:

Configure the Ubuntu operating system to enforce a delay of at least 4 seconds between logon prompts following a failed logon attempt.

Edit the file "/etc/pam.d/common-auth" and set the parameter `pam_faiildelay` to a value of 4000000 or greater:

```
auth required pam_faiildelay.so delay=4000000
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238237
Rule ID: SV-238237r653886_rule
STIG ID: UBTU-20-010075
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.	●	●	●

5.4.22 Ensure PAM prohibits the use of cached authentications after one day (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must be configured such that Pluggable Authentication Module (PAM) prohibits 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.

Audit:

If smart card authentication is not being used on the system, this is Not Applicable. Verify that PAM prohibits the use of cached authentications after one day with the following command:

```
# grep offline_credentials_expiration /etc/sssd/sssd.conf  
/etc/sssd/conf.d/*.conf  
  
offline_credentials_expiration = 1
```

If "offline_credentials_expiration" is not set to a value of "1" in "/etc/sssd/sssd.conf" or in a file with a name ending in .conf in the "/etc/sssd/conf.d/" directory, this is a finding.

Remediation:

Configure PAM 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
```

Note: It is valid for this configuration to be in a file with a name that ends with ".conf" and does not begin with a "." in the "/etc/sssd/conf.d/" directory instead of the "/etc/sssd/sssd.conf" file.

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238362
Rule ID: SV-238362r654261_rule
STIG ID: UBTU-20-010441
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 last successful account logon is displayed upon logon (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must display the date and time of the last successful account logon upon logon

Rationale:

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 users are provided with feedback on when account accesses last occurred.
Check that "pam_lastlog" is used and not silent with the following command:

```
# grep pam_lastlog /etc/pam.d/login
session required pam_lastlog.so showfailed
```

If "pam_lastlog" is missing from "/etc/pam.d/login" file, is not "required", or the "silent" option is present, this is a finding.

Remediation:

Configure the Ubuntu operating system to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/login". Add the following line to the top of "/etc/pam.d/login":

```
session required pam_lastlog.so showfailed
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238373
Rule ID: SV-238373r654294_rule
STIG ID: UBTU-20-010453
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.	●	●	●

5.5 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 minimum days between password changes is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG - Server
- STIG - 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 1 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 1 day):

```
# grep PASS_MIN_DAYS /etc/login.defs  
PASS_MIN_DAYS 1
```

Run the following command and Review list of users and `PAS_MIN_DAYS` to Verify that all users' `PAS_MIN_DAYS` conforms to site policy (no less than 1 day):

```
# awk -F : '(/^[:]+:[^!*]/ && $4 < 1){print $1 " " $4}' /etc/shadow  
No <user>:<PASS_MIN_DAYS> should be returned
```

Remediation:

Set the `PASS_MIN_DAYS` parameter to 1 in `/etc/login.defs`:

```
PASS_MIN_DAYS 1
```

Modify user parameters for all users with a password set to match:

```
# chage --mindays 1 <user>
```

Default Value:

`PASS_MIN_DAYS 0`

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238202
Rule ID: SV-238202r653781_rule
STIG ID: UBTU-20-010007
Severity: CAT III

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.		●	●

5.5.1.2 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.

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. It is recommended that the `PASS_MAX_DAYS` parameter does not exceed 365 days and is greater than the value of `PASS_MIN_DAYS`.

Audit:

Run the following command and verify `PASS_MAX_DAYS` conforms to site policy, does not exceed 365 days, and is greater than `PASS_MIN_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, does not exceed 365 days, and is no less than `PASS_MIN_DAYS`

```
# awk -F: '(/^[:^:]+:[^!*]/ && ($5>365 || $5~/([0-1][-1]\s*/)){print $1 " "  
$5}' /etc/shadow  
  
No <user>:<PASS_MAX_DAYS> should be returned
```

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>
```

Default Value:

`PASS_MAX_DAYS 99999`

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>

Additional Information:

A value of -1 will disable password expiration

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	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.		●	●

5.5.1.3 Ensure password expiration is 60 days or less (Automated)

Profile Applicability:

- STIG - Server
- STIG - 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.

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. It is recommended that the `PASS_MAX_DAYS` parameter does not exceed 60 days and is greater than the value of `PASS_MIN_DAYS`.

Audit:

Run the following command and verify `PASS_MAX_DAYS` conforms to site policy, does not exceed 60 days, and is greater than `PASS_MIN_DAYS`:

```
# grep PASS_MAX_DAYS /etc/login.defs  
PASS_MAX_DAYS 60
```

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, does not exceed 365 days, and is no less than `PASS_MIN_DAYS`

```
# awk -F: '(/^[:^:]+:[^!*]/ && ($5>60 || $5~/([0-1]-1|\s*/)){print $1 " "  
$5}' /etc/shadow  
  
No <user>:<PASS_MAX_DAYS> should be returned
```

Remediation:

Set the `PASS_MAX_DAYS` parameter to conform to site policy in `/etc/login.defs`:

```
PASS_MAX_DAYS 60
```

Modify user parameters for all users with a password set to match:

```
# chage --maxdays 60 <user>
```

Default Value:

`PASS_MAX_DAYS 99999`

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>

Additional Information:

A value of -1 will disable password expiration

The password expiration must be greater than the minimum days between password changes or users will be unable to change their password

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238203
Rule ID: SV-238203r653784_rule
STIG ID: UBTU-20-010008
Severity: CAT III

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 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):

```
# awk -F: '(/^[:]+:[^!*]/ && $6<7) {print $1 " " $6}' /etc/shadow
No <user>:<PASS_WARN_AGE> should be returned
```

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>
```

Default Value:

`PASS_WARN_AGE 7`

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 inactive password lock is 30 days or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG - Server
- STIG - 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):

```
# awk -F: '(/^[:]+:[^!*]/ && ($7~/(\s*|-1)/ || $7>30)) {print $1 " " $7}' /etc/shadow  
No <user>:<INACTIVE> should be returned
```

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>
```

Default Value:

INACTIVE=-1

Additional Information:

A value of -1 would disable this setting

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238330
Rule ID: SV-238330r654165_rule
STIG ID: UBTU-20-010409
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 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

```
# awk -F : '/^[:]+:[^!*]/ {print $1}' /etc/shadow | while read -r usr; do [ "$date --date=$(chage --list "$usr" | grep '^Last password change' | cut -d: -f2)" "+%s" ] -gt "$(date "+%s")" ] && echo "user: $usr password change date: $(chage --list "$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.		●	●

5.5.1.7 Ensure ENCRYPT_METHOD is SHA512 (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

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.

Audit:

Verify that the shadow password suite configuration is set to encrypt passwords with a FIPS 140-2 approved cryptographic hashing algorithm.

Check the hashing algorithm that is being used to hash passwords with the following command:

```
# cat /etc/login.defs | grep -i encrypt_method  
ENCRYPT_METHOD SHA512
```

If "ENCRYPT_METHOD" does not equal SHA512 or greater, this is a finding.

Remediation:

Configure the Ubuntu 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:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238325
Rule ID: SV-238325r654150_rule
STIG ID: UBTU-20-010404
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.	●	●	

5.5.1.8 Ensure root account is locked (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must prevent direct login into the root account.

Rationale:

To assure individual accountability and prevent unauthorized access, organizational users must be individually identified and authenticated.

A group authenticator is a generic account used by multiple individuals. Use of a group authenticator alone does not uniquely identify individual users. Examples of the group authenticator is the UNIX OS "root" user account, the Windows "Administrator" account, the "sa" account, or a "helpdesk" account.

For example, the UNIX and Windows operating systems offer a 'switch user' capability allowing users to authenticate with their individual credentials and, when needed, 'switch' to the administrator role. This method provides for unique individual authentication prior to using a group authenticator.

Users (and any processes acting on behalf of users) need to be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization, which outlines specific user actions that can be performed on the operating system without identification or authentication.

Requiring individuals to be authenticated with an individual authenticator prior to using a group authenticator allows for traceability of actions, as well as adding an additional level of protection of the actions that can be taken with group account knowledge.

Audit:

Verify the Ubuntu operating system prevents direct logins to the root account with the following command:

```
# passwd -S root  
root L 04/23/2020 0 99999 7 -1
```

If the output does not contain "L" in the second field to indicate the account is locked, this is a finding.

Remediation:

Configure the Ubuntu operating system to prevent direct logins to the root account by performing the following operations:

```
# passwd -l root
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238329
Rule ID: SV-238329r654162_rule
STIG ID: UBTU-20-010408
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.	●	●	●

5.5.1.9 Ensure emergency accounts are removed or disabled after 72 hours (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must automatically remove or disable emergency accounts after 72 hours.

Rationale:

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.

Audit:

Verify the Ubuntu operating system expires emergency accounts within 72 hours or less. For every emergency account, run the following command to obtain its account expiration information:

```
# chage -l account_name | grep expires  
Password expires : Aug 07, 2019  
Account expires : Aug 07, 2019
```

Verify each of these accounts has an expiration date set within 72 hours of account creation.

If any of these accounts do not expire within 72 hours of that account's creation, this is a finding.

Remediation:

If an emergency 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 "account_name" with the account to be created.

```
# chage -E $(date -d "+3 days" +%F) account_name
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238331
Rule ID: SV-238331r654168_rule
STIG ID: UBTU-20-010410
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.	●	●	●

5.5.1.10 Ensure immediate change to a permanent password (Manual)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must allow the use of a temporary password for system logons with an immediate change to a permanent password.

Rationale:

Without providing this capability, an account may be created without a password. Non-repudiation cannot be guaranteed once an account is created if a user is not forced to change the temporary password upon initial logon.

Temporary passwords are typically used to allow access when new accounts are created or passwords are changed. It is common practice for administrators to create temporary passwords for user accounts which allow the users to log on, yet force them to change the password once they have successfully authenticated.

Audit:

Verify a policy exists that ensures when a user account is created, it is created using a method that forces a user to change their password upon their next login.
If a policy does not exist, this is a finding.

Remediation:

Create a policy that ensures when a user is created, it is created using a method that forces a user to change their password upon their next login.

Below are two examples of how to create a user account that requires the user to change their password upon their next login.

```
$ sudo chage -d 0 [UserName]
```

OR

```
$ sudo passwd -e [UserName]
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238361
Rule ID: SV-238361r654258_rule
STIG ID: UBTU-20-010440
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.	●	●	●

5.5.1.11 Ensure temporary accounts expiration time of 72 hours or less *(Manual)*

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must provision temporary user accounts 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 operating systems may be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Audit:

Verify that the Ubuntu operating system expires temporary user accounts within 72 hours or less.

For every existing temporary account, run the following command to obtain its account expiration information:

```
# chage -l system_account_name | grep expires  
  
Password expires : Aug 07, 2019  
Account expires : Aug 07, 2019
```

Verify that each of these accounts has an expiration date set within 72 hours of account creation.

If any temporary account does not expire within 72 hours of that account's creation, 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" +%F) system_account_name
```

Additional Information:

```
Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 1 Benchmark Date: 10 Mar 2021  
  
Vul ID: V-238196  
Rule ID: SV-238196r653763_rule  
STIG ID: UBTU-20-010000  
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	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

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|sync|shutdown|halt|^+|) / && $3<"$(awk  
'/^s*UID_MIN/{print $2}' /etc/login.defs)"' &&  
$7!~/((\usr)?\sbin\nologin)/ && $7!~/(\bin)?\false/ {print}' /etc/passwd  
  
# awk -F: '($1!~/root|^+|) / && $3<"$(awk '/^s*UID_MIN/{print $2}'  
/etc/login.defs)"' {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' |  
awk '($2!~/LK?/) {print $1}'
```

Note: The root, sync, shutdown, and halt users are exempted from requiring a non-login shell

Remediation:

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|sync|shutdown|halt|^+)/ && $3<"$(awk  
'/^s*UID_MIN/{print $2}' /etc/login.defs)"' &&  
$7!~/((\usr)?\sbin\nologin)/ && $7!~/(\bin)?\false/ {print $1}'  
/etc/passwd | while read -r user; do usermod -s "$(which nologin)" "$user";  
done
```

The following command will automatically lock not root system accounts:

```
# awk -F: '($1!~/^(root|^+)/ && $3<"$(awk '/^s*UID_MIN/{print $2}'  
/etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' |  
awk '($2~/LK?/) {print $1}' | while read -r user; do usermod -L "$user";  
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.	●	●	●

5.5.3 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	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.	●	●	●

5.5.4 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-----`.

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 `.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/bash.bashrc` - System wide version of `.bashrc`. `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/bash.bashrc*

User Shell Configuration Files:

- `~/.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.

Impact:

Setting **USERGROUPS_ENAB no** in `/etc/login.defs` may change the expected behavior of `useradd` and `userdel`.

Setting **USERGROUPS_ENAB yes** in `/etc/login.defs`

- `userdel` will remove the user's group if it contains no more members
- `useradd` will create by default a group with the name of the user.

Audit:

Run the following to verify:

- A default user umask is set to enforce 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
- 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 -Eqi '^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/bash.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]\b|[0-7]\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/bash.bashrc*
```

No file should be returned

Remediation:

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][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/bash.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 `/etc/pam.d/common-session` 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/bash.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

References:

1. `pam_umask(8)`

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	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.	●	●	●

5.5.5 Ensure default user umask is 077 or more restrictive (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

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.

Impact:

Setting **USERGROUPS_ENAB no** in `/etc/login.defs` may change the expected behavior of `useradd` and `userdel`.

Setting **USERGROUPS_ENAB yes** in `/etc/login.defs`

- `userdel` will remove the user's group if it contains no more members
- `useradd` will create by default a group with the name of the user.

Audit:

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, refer to the remediation procedure below.

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:

Add, uncomment or update the following line:

```
UMASK 077
```

Default Value:

UMASK 022

References:

1. [pam_umask\(8\)](#)

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238209

Rule ID: SV-238209r653802_rule

STIG ID: UBTU-20-010016

Severity: CAT II

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>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.	●	●	●

5.5.6 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/bash.bashrc - System wide version of bash.bashrc. etc/bash.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/bash.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/bash.bashrc ] && BRC="/etc/bash.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 "$output2" ]; then
    echo -e "\\nPASSED\\n\\nTMOUT is configured in: \\\"$output1\\\"\\n"
else
    [ -z "$output1" ] && echo -e "\\nFAILED\\n\\nTMOUT is not configured\\n"
    [ -n "$output2" ] && echo -e "\\nFAILED\\n\\nTMOUT is incorrectly configured in: \\\"$output2\\\"\\n"
fi
```

Remediation:

Review /etc/bash.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/bash.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 are also checked

Other methods of setting a timeout exist not covered here

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.	●	●	●

5.5.7 Ensure default user shell timeout is 600 seconds or less (Automated)

Profile Applicability:

- STIG - Server
- STIG - 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/bash.bashrc - System wide version of bash.bashrc. etc/bash.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/bash.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 600 seconds, to be readonly, to be exported, and is not being changed to a longer timeout.

```
#!/bin/bash

output1="" output2=""
[ -f /etc/bash.bashrc ] && BRC="/etc/bash.bashrc"
for f in "$BRC" /etc/profile /etc/profile.d/*.sh ; do
    grep -Pq '\bTMOUT=(600|[1-5][0-9][0-9]|1-9[0-9]|1-9)\b' "$f" && grep -Pq '\breadonly\h+TMOUT(\h+|\h*;\h*\$|=(600|[1-5][0-9][0-9]|1-9[0-9]|1-9))\b' "$f" && grep -Pq '\bexport\h+([^\n\r]+\h+)\?TMOUT\b' "$f" &&
output1="$f"
done
output2=$(grep -Ps '\bTMOUT=(6[0-9][1-9]|7-9[0-9][0-9]|1-9{3,}0+)\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/bash.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/bash.bashrc

TMOUT configuration examples:

- As multiple lines:

```
TMOUT=600
readonly TMOUT
export TMOUT
```

- As a single line:

```
readonly TMOUT=600 ; 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 are also checked

Other methods of setting a timeout exist not covered here

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238207
Rule ID: SV-238207r653796_rule
STIG ID: UBTU-20-010013
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	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

5.5.8 Ensure vlock is installed (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must allow users to directly initiate a session lock for all connection types.

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 Ubuntu operating systems need to provide users with the ability to manually invoke a session lock so users may secure their session if they need to temporarily vacate the immediate physical vicinity.

Audit:

Verify the "vlock" package is installed by running the following command:

```
# dpkg -l | grep vlock
```

If "vlock" is not installed, this is a finding.

Remediation:

Install the "vlock" package (if it is not already installed) by running the following command:

```
# apt install vlock
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238200
Rule ID: SV-238200r653775_rule
STIG ID: UBTU-20-010005
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	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

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 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 adding, or uncommenting, the `pam_wheel.so` statement in `/etc/pam.d/su`, the `su` command will only allow users in a specific group to execute `su`. This group should be empty to reinforce the use of `sudo` for privileged access.

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 the output matches the line:

```
# grep pam_wheel.so /etc/pam.d/su  
auth required pam_wheel.so use_uid group=<group_name>
```

Run the following command and verify that the group specified in `<group_name>` contains no users:

```
# grep <group_name> /etc/group  
<group_name>:x:<GID>:
```

There should be no users listed after the Group ID field.

Remediation:

Create an empty group that will be specified for use of the `su` command. The group should be named according to site policy.

Example:

```
# groupadd sugroup
```

Add the following line to the `/etc/pam.d/su` file, specifying the empty group:

Example:

```
auth required pam_wheel.so use_uid group=sugroup
```

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 /etc/ssl/certs only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must only allow the use of DoD PKI-established certificate authorities for verification of the establishment of protected sessions.

Rationale:

Untrusted Certificate Authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DoD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DoD-approved CA, trust of this CA has not been established.

The DoD will only accept PKI-certificates obtained from a DoD-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of SSL/TLS certificates.

Audit:

Verify the directory containing the root certificates for the Ubuntu operating system (/etc/ssl/certs) only contains certificate files for DoD PKI-established certificate authorities.

Determine if "/etc/ssl/certs" only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities with the following command:

```
# for f in $(ls /etc/ssl/certs); do openssl x509 -sha256 -in $f -noout -fingerprint | cut -d= -f2 | tr -d ':' | egrep -vw '(9676F287356C89A12683D65234098CB77C4F1C18F23C0E541DE0E196725B7EBE|B107B33F453E5510F68E513110C6F6944BACC263DF0137F821C1B3C2F8F863D2|559A5189452B13F8233F0022363C06F26E3C517C1D4B77445035959DF3244F74|1F4EDE9DC2A241F6521BF518424ACD49EBE84420E69DAF5BAC57AF1F8EE294A9)'; done
```

If any entry is found, this is a finding.

Remediation:

Configure the Ubuntu operating system to only allow the use of DoD PKI-established certificate authorities for verification of the establishment of protected sessions. Edit the "/etc/ca-certificates.conf" file, adding the character "!" to the beginning of all uncommented lines that do not start with the "!" character with the following command:

```
# sed -iE 's/^([#!]+)!/\1/' /etc/ca-certificates.conf
```

Add at least one DoD certificate authority to the "/usr/local/share/ca-certificates" directory in the PEM format.

Update the "/etc/ssl/certs" directory with the following command:

```
# update-ca-certificates
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238364
Rule ID: SV-238364r654267_rule
STIG ID: UBTU-20-010443
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 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 Debian package manager has a number of useful options. One of these, the `--verify` option, can be used to verify that system packages are correctly installed. The `--verify` 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 `dpkg -S` command can be used to determine which package a particular file belongs to. For example the following command determines which package the `/bin/bash` file belongs to:

```
# dpkg -S /bin/bash  
bash: /bin/bash
```

To verify the settings for the package that controls the `/bin/bash` file, run the following:

```
# dpkg --verify bash  
??5?????? c /etc/bash.bashrc
```

Notes:

- 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 assessed 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.

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.

```
# dpkg --verify <package name>
```

Remediation:

Correct any discrepancies found and rerun the audit until output is clean or risk is mitigated or accepted.

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`:

```
# 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 u-x,go-wx /etc/passwd
```

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 command to set permissions on /etc/passwd- :

```
# chown root:root /etc/passwd-
# chmod u-x,go-wx /etc/passwd-
```

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.	●	●	●

6.1.4 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`:

```
# stat /etc/group
Access: (0644/-rw-r--r--)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following command to set permissions on `/etc/group`:

```
# chown root:root /etc/group
# chmod u-x,go-wx /etc/group
```

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.	●	●	●

6.1.5 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-r--r--)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following command to set permissions on /etc/group- :

```
# chown root:root /etc/group-
# chmod u-x,go-wx /etc/group-
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	3.3 Protect Dedicated Assessment Accounts Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.		●	●
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/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 is 0/root, Gid is 0/root or <gid>/shadow, and Access is 640 or more restrictive`:

```
# stat /etc/shadow
Access: (0640/-rw-r-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run **one** of the following commands to set ownership of `/etc/shadow` to `root` and group to either `root` or `shadow`:

```
# chown root:root /etc/shadow
# chown root:shadow /etc/shadow
```

Run the following command to remove excess permissions from `/etc/shadow`:

```
# chmod u-x,g-wx,o-rwx /etc/shadow
```

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.	●	●	●

6.1.7 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 or <gid>/shadow, and Access is 640 or more restrictive:`

```
# stat /etc/shadow-
Access: (0640/-rw-r-----)  Uid: (      0/    root)  Gid: (     42/ shadow)
```

Remediation:

Run **one** of the following commands to set ownership of `/etc/shadow-` to `root` and group to either `root` or `shadow`:

```
# chown root:root /etc/shadow-
# chown root:shadow /etc/shadow-
```

Run the following command to remove excess permissions form `/etc/shadow-:`

```
# chmod u-x,g-wx,o-rwx /etc/shadow-
```

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.	●	●	●

6.1.8 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 or <gid>/shadow, and Access is 640 or more restrictive`:

```
# stat /etc/gshadow
Access: (0640/-rw-r-----)  Uid: (      0/    root)  Gid: (     42/   shadow)
```

Remediation:

Run **one** of the following commands to set ownership of `/etc/gshadow` to `root` and group to either `root` or `shadow`:

```
# chown root:root /etc/gshadow
# chown root:shadow /etc/gshadow
```

Run the following command to remove excess permissions from `/etc/gshadow`:

```
# chmod u-x,g-wx,o-rwx /etc/gshadow
```

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.	●	●	●

6.1.9 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 640 or more restrictive:

```
# stat /etc/gshadow-
Access: (0640/-rw-r-----)  Uid: (      0/    root)  Gid: (     42/   shadow)
```

Remediation:

Run **one** of the following commands to set ownership of /etc/gshadow- to root and group to either root or shadow:

```
# chown root:root /etc/gshadow-
# chown root:shadow /etc/gshadow-
```

Run the following command to remove excess permissions form /etc/gshadow-:

```
# chmod u-x,g-wx,o-rwx /etc/gshadow-
```

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.	●	●	●

6.1.10 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	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.	●	●	●

6.1.11 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	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.	●	●	●

6.1.12 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	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.	●	●	●

6.1.13 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	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.	●	●	●

6.1.14 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	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 Ensure system command files are 0755 or more restrictive (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must have system commands set to a mode of 0755 or less permissive.

Rationale:

If the Ubuntu 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 Ubuntu operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must 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:

```
/bin  
/sbin  
/usr/bin  
/usr/sbin  
/usr/local/bin  
/usr/local/sbin
```

Check that the system command files have mode 0755 or less permissive with the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm  
/022 -type f -exec stat -c "%n %a" '{}' \;
```

If any files 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:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm /022 -type f -exec chmod 755 '{}' \;
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238376
Rule ID: SV-238376r654303_rule
STIG ID: UBTU-20-010456
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.	●	●	●

6.1.16 Ensure system command files are owned by root (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must have system commands owned by root.

Rationale:

If the Ubuntu 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 Ubuntu operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must 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:

```
/bin  
/sbin  
/usr/bin  
/usr/sbin  
/usr/local/bin  
/usr/local/sbin
```

Use the following command for the check:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -user  
root -type f -exec stat -c "%n %U" '{}' \;
```

If any system commands are returned, this is a finding.

Remediation:

Configure the system commands and their respective parent directories to be protected from unauthorized access. Run the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -user root -type f -exec chown root '{}' \;
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238377
Rule ID: SV-238377r654306_rule
STIG ID: UBTU-20-010457
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.	●	●	●

6.1.17 Ensure system command files are group-owned by root (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must have system commands group-owned by root.

Rationale:

If the Ubuntu 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 Ubuntu operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must 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:

```
/bin  
/sbin  
/usr/bin  
/usr/sbin  
/usr/local/bin  
/usr/local/sbin
```

Run the check with the following command:

```
# find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -  
group root -type f -exec stat -c "%n %G" '{}' \;
```

If any system commands are returned that are not Set Group ID up on execution (SGID) files and owned by a privileged account, this is a finding.

Remediation:

Configure the system commands to be protected from unauthorized access. Run the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -group root -type f ! -perm /2000 -exec chgrp root '{}' \;
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238378
Rule ID: SV-238378r654309_rule
STIG ID: UBTU-20-010458
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 directories that contain system commands set to 0755 or more restrictive (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must have directories that contain system commands set to 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.

Operating 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 has in order to make access decisions regarding the deletion of 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 system commands directories have mode 0755 or less permissive:

```
/bin  
/sbin  
/usr/bin  
/usr/sbin  
/usr/local/bin  
/usr/local/sbin
```

Check that the system command directories have mode 0755 or less permissive with the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm  
/022 -type d -exec stat -c "%n %a" '{}' \;
```

If any directories are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the system commands directories to be protected from unauthorized access. Run the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm /022 -type d -exec chmod -R 755 '{}' \\;
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238344
Rule ID: SV-238344r654207_rule
STIG ID: UBTU-20-010423
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 directories that contain system commands are owned by root (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must have directories that contain system commands 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.

Operating 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 has in order to make access decisions regarding the deletion of 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 system commands directories are owned by root:

```
/bin  
/sbin  
/usr/bin  
/usr/sbin  
/usr/local/bin  
/usr/local/sbin
```

Use the following command for the check:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -user  
root -type d -exec stat -c "%n %U" '{}' \;
```

If any system commands directories are returned, this is a finding.

Remediation:

Configure the system commands directories to be protected from unauthorized access. Run the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -user root -type d -exec chown root '{}' \;
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238345
Rule ID: SV-238345r654210_rule
STIG ID: UBTU-20-010424
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 directories that contain system commands are group-owned by root (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system must have directories that contain system commands 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.

Operating 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 has in order to make access decisions regarding the deletion of 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:

Check Text: Verify the system commands directories are group-owned by root:

```
/bin  
/sbin  
/usr/bin  
/usr/sbin  
/usr/local/bin  
/usr/local/sbin
```

Run the check with the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -group  
root -type d -exec stat -c "%n %G" '{}' \;
```

If any system commands directories are returned that are not Set Group ID up on execution (SGID) files and owned by a privileged account, this is a finding.

Remediation:

Configure the system commands directories to be protected from unauthorized access. Run the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -group root -type d -exec chgrp root '{}' \;
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238346
Rule ID: SV-238346r654213_rule
STIG ID: UBTU-20-010425
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 system library files are 0755 or more restrictive (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system 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 which execute with escalated privileges. Only qualified and authorized individuals must 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 directories "/lib", "/lib64", and "/usr/lib" have mode 0755 or less permissive with the following command:

```
# find /lib /lib64 /usr/lib -perm /022 -type f -exec stat -c "%n %a" '{}' \;
/usr/lib64/pkcs11-spy.so
```

If any files are 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:

```
# find /lib /lib64 /usr/lib -perm /022 -type f -exec chmod 755 '{}' \;
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238347
Rule ID: SV-238347r654216_rule
STIG ID: UBTU-20-010426
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 system library files are owned by root (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system operating system 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 which execute with escalated privileges. Only qualified and authorized individuals must 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 directories "/lib", "/lib64", and "/usr/lib" are owned by root with the following command:

```
# find /lib /usr/lib /lib64 ! -user root -type f -exec stat -c "%n %U" '{}' \;
```

If any system-wide library file is returned, this is a finding.

Remediation:

Configure the system library files to be protected from unauthorized access. Run the following command:

```
# find /lib /usr/lib /lib64 ! -user root -type f -exec chown root '{}' \;
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238349
Rule ID: SV-238349r654222_rule
STIG ID: UBTU-20-010428
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 system library files are group-owned by root (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system operating system library files must be group-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 which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide library files contained in the directories "/lib", "/lib64", and "/usr/lib" are group-owned by root with the following command:

```
# find /lib /usr/lib /lib64 ! -group root -type f -exec stat -c "%n %G" '{}' \;
```

If any system-wide shared library file is returned, this is a finding.

Remediation:

Configure the system library files to be protected from unauthorized access. Run the following command:

```
# find /lib /usr/lib /lib64 ! -group root -type f -exec chgrp root '{}' \;
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238351
Rule ID: SV-238351r654228_rule
STIG ID: UBTU-20-010430
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 system library directories are 0755 or more restrictive (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system library directories 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 which execute with escalated privileges. Only qualified and authorized individuals must 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 directories "/lib", "/lib64", and "/usr/lib" have mode 0755 or less permissive with the following command:

```
# find /lib /lib64 /usr/lib -perm /022 -type d -exec stat -c "%n %a" '{}' \;
```

If any of the aforementioned directories are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the shared library directories to be protected from unauthorized access. Run the following command:

```
# find /lib /lib64 /usr/lib -perm /022 -type d -exec chmod 755 '{}' \;
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238348
Rule ID: SV-238348r654219_rule
STIG ID: UBTU-20-010427
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 system library directories are owned by root (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system library directories 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 which execute with escalated privileges. Only qualified and authorized individuals must 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 directories "/lib", "/lib64", and "/usr/lib" are owned by root with the following command:

```
# find /lib /usr/lib /lib64 ! -user root -type d -exec stat -c "%n %U" '{}' \;
```

If any system-wide library directory is returned, this is a finding.

Remediation:

Configure the library files and their respective parent directories to be protected from unauthorized access. Run the following command:

```
# find /lib /usr/lib /lib64 ! -user root -type d -exec chown root '{}' \;
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238350
Rule ID: SV-238350r654225_rule
STIG ID: UBTU-20-010429
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 system library directories are group-owned by root (Automated)

Profile Applicability:

- STIG - Server
- STIG - Workstation

Description:

The operating system library directories must be group-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 which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide library directories "/lib", "/lib64", and "/usr/lib" are group-owned by root with the following command:

```
# find /lib /usr/lib /lib64 ! -group root -type d -exec stat -c "%n %G" '{}' \;
```

If any system-wide shared library directory is returned, this is a finding.

Remediation:

Configure the system library directories to be protected from unauthorized access. Run the following command:

```
# find /lib /usr/lib /lib64 ! -group root -type d -exec chgrp root '{}' \;
```

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238352
Rule ID: SV-238352r654231_rule
STIG ID: UBTU-20-010431
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 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 accounts in /etc/passwd use shadowed passwords (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Local accounts can use shadowed passwords. With shadowed passwords, the passwords are saved in shadow password file, `/etc/shadow`, encrypted by a salted one-way hash. Accounts with a shadowed password have an `x` in the second field in `/etc/passwd`.

Rationale:

The `/etc/passwd` file also contains information like user ID's and group ID's that are used by many system programs. Therefore, the `/etc/passwd` file must remain world readable. In spite of encoding the password with a randomly-generated one-way hash function, an attacker could still break the system if they got access to the `/etc/passwd` file. This can be mitigated by using shadowed passwords, thus moving the passwords in the `/etc/passwd` file to `/etc/shadow`. The `/etc/shadow` file is set so only root will be able to read and write. This helps mitigate the risk of an attacker gaining access to the encoded passwords with which to perform a dictionary attack.

Notes:

- *All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.*
- *A user account with an empty second field in /etc/passwd allows the account to be logged into by providing only the username.*

Audit:

Run the following command and verify that no output is returned:

```
# awk -F: '($2 != "x" ) { print $1 " is not set to shadowed passwords "}'  
/etc/passwd
```

Remediation:

Run the following command to set accounts to use shadowed passwords:

```
# sed -e 's/^([a-zA-Z0-9_]*):[^:]*:\1:x:/' -i /etc/passwd
```

Investigate to determine if the account is logged in and 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	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.		●	●

6.2.2 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.		●	●

6.2.3 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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.4 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.

Note: The audit script checks all users with interactive shells except `halt`, `sync`, `shutdown`, and `nfsnobody`

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
```

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)/ &&
$7!~(^(/\usr)?/\sbin\nologin(/)?$/ && $7!~(^(/\usr)?/\bin\nfalse(/)?$/) {
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
```

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.	●	●	●

6.2.5 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)/ && $7!~/^(\//usr)?\sbin\\nologin(\//)?$/ && $7!~/(\//usr)?\bin\\false(\//)?$/) { 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)/ && $7!~/^(\//usr)?\sbin\!/nologin(\//)?$/ && $7!~/^(\/usr)?\bin\!false(\//)?$/) { 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.	●	●	●

6.2.6 Ensure users' home directories permissions are 750 or more restrictive (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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)/ && $7!~/^(\//usr)?\!/sbin\!/nologin(\//)?$/ && $7!~/^(\/usr)?\!/bin\!/false(\//)?$/) {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)/ && $7!~/^(\//usr)?\sbin\!/nologin(\//)?$/ && $7!~/(\//usr)?\bin\!/false(\//)?$/) {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
```

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.	●	●	●

6.2.7 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)/ && $7!~/^(\//usr)?\!/sbin\!/nologin(\//)?$/ && $7!~/(\//usr)?\!/bin\!/false(\//)?$/) { 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)/ && $7!~/^(\//usr)?\sbin\nologin(\//)?$/ && $7!~/(\//usr)?\bin\n/false(\//)?$/) { 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 "$fileperm" | cut -c9)" != "-" ]; then
                    chmod go-w "$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.	●	●	●

6.2.8 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.

While the system administrator can establish secure permissions for users' `.netrc` files, the users can easily override these.

Note: While the complete removal of `.netrc` files is recommended, if any are required on the system secure permissions must be applied.

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)/ && $7~/^(\!/usr)?\!/sbin\!/nologin(\!)?$/ && $7~/^(\/usr)?\!/bin\!/false(\!)?$/) { 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` file permissions and determine the action to be taken in accordance with local site policy.

The following script will remove `.netrc` files from interactive users' home directories

```
#!/bin/bash

awk -F: '$1!~/\(\ halt|sync|shutdown\)/ && $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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.9 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 lines are returned:

```
#!/bin/bash

awk -F: '($1!~/(root|halt|sync|shutdown)/ &&
$7!~/^(\/usr)?\/sbin\/nologin(\/)?$/ && $7!~/^(\/usr)?\/bin\/false(\/)?$/) {
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)/ &&
$7!~(^(\!/usr)?\!/sbin\!/nologin(\!)?$/ && $7!~(\!/usr)?\!/bin\!/false(\!)?$/) {'
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.	●	●	●

6.2.10 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 lines are returned:

```
#!/bin/bash

awk -F: '$(1!~/^(root|halt|sync|shutdown)/ &&
$7!~/^(\/usr)?\/sbin\/nologin()?$/. && $7!~/^(\/usr)?\/bin\/false()?$/) {'
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
  if [ -d "$dir" ]; then
    file="$dir/.rhosts"
    if [ ! -h "$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)/ &&
$7!~/^(\//usr)?\sbin\nologin(\//)?$/ && $7!~/(\//usr)?\bin/false(\//)?$/ {'
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
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.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.2.11 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 Item 5.6 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	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> 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	<u>4.6 Use of Dedicated Machines For All Administrative Tasks</u> Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.			●

6.2.12 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.	●	●	●

6.2.13 Ensure no duplicate UIDs exist (Automated)

Profile Applicability:

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

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:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide
Version 1, Release: 1 Benchmark Date: 10 Mar 2021

Vul ID: V-238205
Rule ID: SV-238205r653790_rule
STIG ID: UBTU-20-010010
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.		●	●

6.2.14 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	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.	●	●	●

6.2.15 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 -r 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	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.	●	●	●

6.2.16 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	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.	●	●	●

6.2.17 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.	●	●	●

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 freevxfs filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure mounting of jffs2 filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure mounting of hfs filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.5	Ensure mounting of hfsplus filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.6	Ensure mounting of squashfs filesystems is disabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.7	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 /dev/shm is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Ensure nodev option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Ensure nosuid option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Ensure noexec option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Ensure separate partition exists for /var (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.11	Ensure separate partition exists for /var/tmp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.12	Ensure /var/tmp partition includes the nodev option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.13	Ensure /var/tmp partition includes the nosuid option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.14	Ensure /var/tmp partition includes the noexec option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.15	Ensure separate partition exists for /var/log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

1.1.16	Ensure separate partition exists for /var/log/audit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.17	Ensure separate partition exists for /home (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.18	Ensure /home partition includes the nodev option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.19	Ensure nodev option set on removable media partitions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.20	Ensure nosuid option set on removable media partitions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.21	Ensure noexec option set on removable media partitions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.22	Ensure sticky bit is set on all world-writable directories (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.23	Disable Automounting (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.24	Disable USB Storage (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.25	Ensure data-at-rest encryption is enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.26	Ensure data-at-rest employs cryptographic mechanisms to prevent unauthorized modification (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.27	Ensure data-at-rest employs cryptographic mechanisms to prevent unauthorized disclosure (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Configure Software Updates		
1.2.1	Ensure package manager repositories are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Ensure GPG keys are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Ensure apt is configured to prevent installation without verification of a recognized and approved digital signature (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Ensure the Advance Package Tool removes all software components after updated versions have been installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Filesystem Integrity Checking		
1.3.1	Ensure AIDE is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Ensure filesystem integrity is regularly checked (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.3	Ensure System Administrator are notified of changes to the baseline configuration or anomalies (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Ensure aide script to check file integrity is the default (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	Secure Boot Settings		
1.4.1	Ensure permissions on bootloader config are not overridden (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure bootloader password is set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Ensure permissions on bootloader config are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

1.4.4	Ensure authentication required for single user mode (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.5	Additional Process Hardening		
1.5.1	Ensure XD/NX support is enabled (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.5.2	Ensure address space layout randomization (ASLR) is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.5.3	Ensure prelink is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.5.4	Ensure core dumps are restricted (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.5.5	Ensure maxlogins is 10 or less (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.5.6	Ensure kdump service is not enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.5.7	Ensure FIPS mode is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.5.8	Ensure the Ctrl-Alt-Delete key sequence is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.6	Mandatory Access Control		
1.6.1	Configure AppArmor		
1.6.1.1	Ensure AppArmor is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.6.1.2	Ensure AppArmor is installed, enabled, and active (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.6.1.3	Ensure AppArmor is enabled in the bootloader configuration (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.6.1.4	Ensure all AppArmor Profiles are in enforce or complain mode (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.6.1.5	Ensure all AppArmor Profiles are enforcing (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.7	Command Line Warning Banners		
1.7.1	Ensure message of the day is configured properly (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.7.2	Ensure local login warning banner is configured properly (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.7.3	Ensure remote login warning banner is configured properly (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.7.4	Ensure permissions on /etc/motd are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.7.5	Ensure permissions on /etc/issue are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.7.6	Ensure permissions on /etc/issue.net are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.8	GNOME Display Manager		
1.8.1	Ensure GNOME Display Manager is removed (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.8.2	Ensure GDM login banner is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.8.3	Ensure disable-user-list is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.8.4	Ensure XDCMP is not enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.8.5	Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

1.8.6	Ensure user's session lock is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.8.7	Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.9	Ensure updates, patches, and additional security software are installed (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Services		
2.1	Special Purpose Services		
2.1.1	Time Synchronization		
2.1.1.1	Ensure time synchronization is in use (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.1.2	Ensure systemd-timesyncd is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.1.3	Ensure chrony is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.1.4	Ensure ntp is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.1.5	Ensure system timezone is set to UTC or GMT (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.1.6	Ensure system clocks are synchronized with a time server designated for the appropriate DoD network (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.1.7	Ensure system clocks are synchronize to the authoritative time source when the time difference is greater than one second (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.2	Ensure X Window System is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.3	Ensure Avahi Server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.4	Ensure CUPS is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.5	Ensure DHCP Server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.6	Ensure LDAP server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.7	Ensure NFS is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.8	Ensure DNS Server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.9	Ensure FTP Server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.10	Ensure HTTP server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.11	Ensure IMAP and POP3 server are not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.12	Ensure Samba is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.13	Ensure HTTP Proxy Server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.14	Ensure SNMP Server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.15	Ensure mail transfer agent is configured for local-only mode (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.16	Ensure rsync service is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.17	Ensure NIS Server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.18	Ensure telnetd is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.19	Ensure rsh-server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.20	Ensure Endpoint Security for Linux Threat Prevention is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2	Service Clients		
2.2.1	Ensure NIS Client is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.2	Ensure rsh client is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.3	Ensure talk client is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

2.2.4	Ensure telnet client is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.5	Ensure LDAP client is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.6	Ensure RPC is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.3	Ensure nonessential services are removed or masked (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Network Configuration		
3.1	Disable unused network protocols and devices		
3.1.1	Disable IPv6 (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.1.2	Ensure wireless interfaces are disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.2	Network Parameters (Host Only)		
3.2.1	Ensure packet redirect sending is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.2.2	Ensure IP forwarding is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3	Network Parameters (Host and Router)		
3.3.1	Ensure source routed packets are not accepted (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.2	Ensure ICMP redirects are not accepted (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.3	Ensure secure ICMP redirects are not accepted (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.4	Ensure suspicious packets are logged (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.5	Ensure broadcast ICMP requests are ignored (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.6	Ensure bogus ICMP responses are ignored (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.7	Ensure Reverse Path Filtering is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.8	Ensure TCP SYN Cookies is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.9	Ensure IPv6 router advertisements are not accepted (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4	Uncommon Network Protocols		
3.4.1	Ensure DCCP is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.2	Ensure SCTP is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.3	Ensure RDS is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.4	Ensure TIPC is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5	Firewall Configuration		
3.5.1	Configure UncomplicatedFirewall		
3.5.1.1	Ensure ufw is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.1.2	Ensure iptables-persistent is not installed with ufw (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.1.3	Ensure ufw service is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.1.4	Ensure ufw loopback traffic is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.1.5	Ensure ufw outbound connections are configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.1.6	Ensure ufw firewall rules exist for all open ports (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.1.7	Ensure ufw default deny firewall policy (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.1.8	Ensure functions, ports, protocols, and services are restricted (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.1.9	Ensure UFW rate-limits impacted network interfaces (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.2	Configure nftables		

3.5.2.1	Ensure nftables is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.2.2	Ensure ufw is uninstalled or disabled with nftables (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.2.3	Ensure iptables are flushed with nftables (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.2.4	Ensure a nftables table exists (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.2.5	Ensure nftables base chains exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.2.6	Ensure nftables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.2.7	Ensure nftables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.2.8	Ensure nftables default deny firewall policy (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.2.9	Ensure nftables service is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.2.10	Ensure nftables rules are permanent (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.3	Configure iptables		
3.5.3.1	Configure iptables software		
3.5.3.1.1	Ensure iptables packages are installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.3.1.2	Ensure nftables is not installed with iptables (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.3.1.3	Ensure ufw is uninstalled or disabled with iptables (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.3.2	Configure IPv4 iptables		
3.5.3.2.1	Ensure iptables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.3.2.2	Ensure iptables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.3.2.3	Ensure iptables default deny firewall policy (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.3.2.4	Ensure iptables firewall rules exist for all open ports (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.3.3	Configure IPv6 ip6tables		
3.5.3.3.1	Ensure ip6tables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.3.3.2	Ensure ip6tables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.3.3.3	Ensure ip6tables default deny firewall policy (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.5.3.3.4	Ensure ip6tables firewall rules exist for all open ports (Automated)	<input type="checkbox"/>	<input checked="" 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 checked="" type="checkbox"/>
4.1.1.2	Ensure auditd service is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.1.4	Ensure audit_backlog_limit is sufficient (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.2	Configure Data Retention		
4.1.2.1	Ensure audit log storage size is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4.1.2.2	Ensure audit logs are not automatically deleted (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.2.3	Ensure system is disabled when audit logs are full (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.2.4	Ensure shut down by default upon audit failure (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.2.5	Ensure sufficient storage capacity to store at least one week worth of audit records (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.2.6	Ensure audit event multiplexor is configured to off-load audit logs onto a different system or storage media from the system being audited (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.2.7	Ensure security personnel are notified when storage volume reaches 75 percent utilization (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.2.8	Ensure crontab script running to offload audit events of standalone systems (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3	Configure auditd rules		
4.1.3.1	Ensure events that modify date and time information are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.2	Ensure kernel module loading and unloading is collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.3	Ensure system administrator command executions (sudo) are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.4	Ensure changes to system administration scope (sudoers) is collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.5	Ensure file deletion events by users are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.6	Ensure successful file system mounts are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.7	Ensure use of privileged commands is collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.8	Ensure unsuccessful unauthorized file access attempts are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.9	Ensure discretionary access control permission modification events are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.10	Ensure session initiation information is collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.11	Ensure login and logout events are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.12	Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.13	Ensure events that modify the system's network environment are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.14	Ensure events that modify user/group information are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4.1.3.15	Ensure successful and unsuccessful uses of the su command are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.16	Ensure successful and unsuccessful uses of the chfn command are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.17	Ensure successful and unsuccessful uses of the ssh-agent command are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.18	Ensure successful and unsuccessful uses of the ssh-keysign command are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.19	Ensure successful and unsuccessful attempts to use the setattr system call are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.20	Ensure successful and unsuccessful attempts to use the lsetattr system call are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.21	Ensure successful and unsuccessful attempts to use the fsetattr system call are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.22	Ensure successful and unsuccessful attempts to use the removexattr system call are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.23	Ensure successful and unsuccessful attempts to use the fremovexattr system call are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.24	Ensure successful and unsuccessful attempts to use the lremovexattr system call are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.25	Ensure successful and unsuccessful uses of the open_by_handle_at system call are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.26	Ensure successful and unsuccessful uses of the sudo command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.27	Ensure successful and unsuccessful attempts to use the sudoedit command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.28	Ensure successful and unsuccessful attempts to use the chsh command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.29	Ensure successful and unsuccessful attempts to use the newgrp command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.30	Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.31	Ensure successful and unsuccessful attempts to use the apparmor_parser command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.32	Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.33	Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.34	Ensure successful and unsuccessful attempts to use the passwd command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.35	Ensure successful and unsuccessful attempts to use the unix_update command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.36	Ensure successful and unsuccessful attempts to use the gpasswd command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

4.1.3.37	Ensure successful and unsuccessful attempts to use the chage command are recorded (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.38	Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.39	Ensure successful and unsuccessful attempts to use the crontab command are recorded (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.40	Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are recorded (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.41	Ensure successful and unsuccessful uses of the finit_module syscall are recorded (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.42	Ensure execution of privileged functions is recorded (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.43	Ensure nonlocal administrative access events are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.44	Ensure successful and unsuccessful attempts to use the kmod command are recorded (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.45	Ensure successful and unsuccessful attempts to use the fdisk command are recorded (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.46	Ensure the audit configuration is immutable (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.4	Configure auditd file access		
4.1.4.1	Ensure audit log files are not read or write-accessible by unauthorized users (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.4.2	Ensure only authorized users own audit log files (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.4.3	Ensure only authorized groups ownership of audit log files (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.4.4	Ensure the audit log directory is 0750 or more restrictive (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.4.5	Ensure audit configuration files are 0640 or more restrictive (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.4.6	Ensure only authorized accounts own the audit configuration files (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.4.7	Ensure only authorized groups own the audit configuration files (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.4.8	Ensure audit tools are mode of 0755 or more restrictive (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.4.9	Ensure audit tools are owned by root (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.4.10	Ensure audit tools are group-owned by root (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.4.11	Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2	Configure Logging		
4.2.1	Configure rsyslog		
4.2.1.1	Ensure rsyslog is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.1.2	Ensure rsyslog Service is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4.2.1.3	Ensure logging is configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.1.4	Ensure rsyslog default file permissions configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.1.5	Ensure rsyslog is configured to send logs to a remote log host (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.1.6	Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.1.7	Ensure remote access methods are monitored (Automated)	<input type="checkbox"/>	<input checked="" 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 checked="" type="checkbox"/>
4.2.2.2	Ensure journald is configured to compress large log files (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.3	Ensure logrotate is configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.4	Ensure logrotate assigns appropriate permissions (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.5	Ensure permissions on all logfiles are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.6	Ensure /var/log is group-owned by syslog (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.7	Ensure /var/log is owned by root (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.8	Ensure /var/log/syslog is group-owned by adm (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.9	Ensure /var/log/syslog is owned by syslog (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.10	Ensure /var/log/syslog is 0640 or more restrictive (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5	Access, Authentication and Authorization		
5.1	Configure time-based job schedulers		
5.1.1	Ensure cron daemon is enabled and running (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.2	Ensure permissions on /etc/crontab are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.4	Ensure permissions on /etc/cron.daily are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.7	Ensure permissions on /etc/cron.d are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.8	Ensure cron is restricted to authorized users (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

5.1.9	Ensure at is restricted to authorized users (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2	Configure sudo		
5.2.1	Ensure sudo is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.2	Ensure sudo commands use pty (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.3	Ensure sudo log file exists (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.4	Ensure only users who need access to security functions are part of sudo group (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.5	Ensure users must reauthenticate for privilege escalation or when changing roles (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3	Configure SSH Server		
5.3.1	Ensure SSH is installed and active (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.2	Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.3	Ensure permissions on SSH private host key files are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.4	Ensure permissions on SSH public host key files are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.5	Ensure SSH access is limited (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.6	Ensure SSH LogLevel is appropriate (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.7	Ensure SSH X11 forwarding is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.8	Ensure SSH MaxAuthTries is set to 4 or less (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.9	Ensure SSH IgnoreRhosts is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.10	Ensure SSH HostbasedAuthentication is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.11	Ensure SSH root login is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.12	Ensure SSH PermitEmptyPasswords is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.13	Ensure SSH PermitUserEnvironment is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.14	Ensure only strong Ciphers are used (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.15	Ensure only FIPS 140-2 approved Ciphers are used (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.16	Ensure only strong MAC algorithms are used (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.17	Ensure only FIPS 140-2 approved MAC algorithms are used (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.18	Ensure only strong Key Exchange algorithms are used (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.19	Ensure SSH Idle Timeout Interval is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.20	Ensure SSH LoginGraceTime is set to one minute or less (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.21	Ensure SSH warning banner is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.22	Ensure SSH PAM is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.23	Ensure SSH AllowTcpForwarding is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

5.3.24	Ensure SSH MaxStartups is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.25	Ensure SSH MaxSessions is limited (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.26	Ensure network connections associated with SSH traffic are terminated after a period of inactivity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.27	Ensure network connections associated with SSH traffic are terminated at the end of the session or 10 minutes of inactivity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.28	Ensure Standard Mandatory DoD Notice and Consent Banner displayed before granting any local or remote connection to the system (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.29	Ensure X11UseLocalhost is enabled (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 new and changed passwords use pwquality (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3	Ensure lockout for failed password attempts is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.4	Ensure password reuse is limited (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.5	Ensure password hashing algorithm is SHA-512 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.6	Ensure password is at least 15 characters (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.7	Ensure password includes at least one upper-case character (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.8	Ensure password includes at least one lower-case character (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.9	Ensure password includes at least one numeric character (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.10	Ensure password includes at least one special character (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.11	Ensure passwords can not use dictionary words (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.12	Ensure change of at least 8 characters when passwords are changed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.13	Ensure lockout for failed password attempts until the locked account is released (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.14	Ensure the libpam-pkcs11 package is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.15	Ensure the opensc-pkcs11 is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.16	Ensure authenticated identity is mapped to the user or group account for PKI-based authentication (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.17	Ensure smart card logins for multifactor authentication for local and network access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.18	Ensure certificates are validated by constructing a certification path to an accepted trust anchor (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

5.4.19	Ensure Personal Identity Verification credentials are electronically verified (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.20	Ensure PKI local cache of revocation data (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.21	Ensure logging delay after failed logon attempt (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.22	Ensure PAM prohibits the use of cached authentications after one day (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.23	Ensure last successful account logon is displayed upon logon (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 minimum days between password changes is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.2	Ensure password expiration is 365 days or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.3	Ensure password expiration is 60 days or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.4	Ensure password expiration warning days is 7 or more (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.5	Ensure inactive password lock is 30 days or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.6	Ensure all users last password change date is in the past (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.7	Ensure ENCRYPT_METHOD is SHA512 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.8	Ensure root account is locked (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.9	Ensure emergency accounts are removed or disabled after 72 hours (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.10	Ensure immediate change to a permanent password (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.11	Ensure temporary accounts expiration time of 72 hours or less (Manual)	<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 group for the root account is GID 0 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.4	Ensure default user umask is 027 or more restrictive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.5	Ensure default user umask is 077 or more restrictive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.6	Ensure default user shell timeout is 900 seconds or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.7	Ensure default user shell timeout is 600 seconds or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.8	Ensure vlock is installed (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 access to the su command is restricted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

5.8	Ensure /etc/ssl/certs only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6	System Maintenance		
6.1	System File Permissions		
6.1.1	Audit system file permissions (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.2	Ensure permissions on /etc/passwd are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.3	Ensure permissions on /etc/passwd- are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.4	Ensure permissions on /etc/group are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.5	Ensure permissions on /etc/group- are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.6	Ensure permissions on /etc/shadow are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.7	Ensure permissions on /etc/shadow- are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.8	Ensure permissions on /etc/gshadow are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.9	Ensure permissions on /etc/gshadow- are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.10	Ensure no world writable files exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.11	Ensure no unowned files or directories exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.12	Ensure no ungrouped files or directories exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.13	Audit SUID executables (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.14	Audit SGID executables (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.15	Ensure system command files are 0755 or more restrictive (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.16	Ensure system command files are owned by root (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.17	Ensure system command files are group-owned by root (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.18	Ensure directories that contain system commands set to 0755 or more restrictive (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.19	Ensure directories that contain system commands are owned by root (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.20	Ensure directories that contain system commands are group-owned by root (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.21	Ensure system library files are 0755 or more restrictive (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.22	Ensure system library files are owned by root (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.23	Ensure system library files are group-owned by root (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

6.1.24	Ensure system library directories are 0755 or more restrictive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.25	Ensure system library directories are owned by root (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.26	Ensure system library directories are group-owned by root (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2	User and Group Settings		
6.2.1	Ensure accounts in /etc/passwd use shadowed passwords (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2	Ensure password fields are not empty (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Ensure all groups in /etc/passwd exist in /etc/group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Ensure all users' home directories exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure users own their home directories (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure users' home directories permissions are 750 or more restrictive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure users' dot files are not group or world writable (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure no users have .netrc files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.9	Ensure no users have .forward files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.10	Ensure no users have .rhosts files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.11	Ensure root is the only UID 0 account (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.12	Ensure root PATH Integrity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.13	Ensure no duplicate UIDs exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.14	Ensure no duplicate GIDs exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.15	Ensure no duplicate user names exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.16	Ensure no duplicate group names exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.17	Ensure shadow group is empty (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
Jul 26, 2021	1.0.0	Published