



DRAFT CIS Ubuntu Linux 22.04 LTS Benchmark

v1.0.0 - 07-18-2022

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/>

DRAFT

Table of Contents

Terms of Use	1
Table of Contents.....	2
Overview.....	13
Intended Audience.....	13
Typographical Conventions.....	15
Recommendation Definitions.....	16
Title.....	16
Assessment Status.....	16
Automated	16
Manual.....	16
Profile	16
Description.....	16
Rationale Statement	16
Impact Statement.....	17
Audit Procedure.....	17
Remediation Procedure.....	17
Default Value.....	17
References	17
CIS Critical Security Controls® (CIS Controls®).....	17
Additional Information.....	17
Profile Definitions	18
Acknowledgements	19
Recommendations	20
1 Initial Setup	21
1.1 Filesystem Configuration.....	22
1.1.1 Disable unused filesystems	23
Start up scripts	23
Return values.....	23
1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated)	24
1.1.1.2 Ensure mounting of squashfs filesystems is disabled (Automated)	26
1.1.1.3 Ensure mounting of udf filesystems is disabled (Automated)	29
1.1.2 Configure /tmp	32
1.1.2.1 Ensure /tmp is a separate partition (Automated).....	33
1.1.2.2 Ensure nodev option set on /tmp partition (Automated)	36
1.1.2.3 Ensure noexec option set on /tmp partition (Automated)	38
1.1.2.4 Ensure nosuid option set on /tmp partition (Automated)	40
1.1.3 Configure /var	42

1.1.3.1 Ensure separate partition exists for /var (Automated)	43
Protection from resource exhaustion	43
Fine grained control over the mount.....	43
Protection from exploitation	43
1.1.3.2 Ensure nodev option set on /var partition (Automated)	45
1.1.3.3 Ensure noexec option set on /var partition (Automated)	47
1.1.3.4 Ensure nosuid option set on /var partition (Automated)	49
1.1.4 Configure /var/tmp	51
1.1.4.1 Ensure separate partition exists for /var/tmp (Automated)	52
Protection from resource exhaustion	52
Fine grained control over the mount.....	52
Protection from exploitation	52
1.1.4.2 Ensure noexec option set on /var/tmp partition (Automated)	54
1.1.4.3 Ensure nosuid option set on /var/tmp partition (Automated)	56
1.1.4.4 Ensure nodev option set on /var/tmp partition (Automated)	58
1.1.5 Configure /var/log.....	60
1.1.5.1 Ensure separate partition exists for /var/log (Automated)	61
Protection from resource exhaustion	61
Fine grained control over the mount.....	61
Protection of log data	61
1.1.5.2 Ensure nodev option set on /var/log partition (Automated)	63
1.1.5.3 Ensure noexec option set on /var/log partition (Automated)	65
1.1.5.4 Ensure nosuid option set on /var/log partition (Automated)	67
1.1.6 Configure /var/log/audit	69
1.1.6.1 Ensure separate partition exists for /var/log/audit (Automated)	70
Protection from resource exhaustion	70
Fine grained control over the mount.....	70
Protection of audit data	70
1.1.6.2 Ensure noexec option set on /var/log/audit partition (Automated)	72
1.1.6.3 Ensure nodev option set on /var/log/audit partition (Automated)	74
1.1.6.4 Ensure nosuid option set on /var/log/audit partition (Automated)	76
1.1.7 Configure /home.....	78
1.1.7.1 Ensure separate partition exists for /home (Automated)	79
Protection from resource exhaustion	79
Fine grained control over the mount.....	79
Protection of user data	79
1.1.7.2 Ensure nodev option set on /home partition (Automated)	81
1.1.7.3 Ensure nosuid option set on /home partition (Automated)	83
1.1.7.4 Ensure usrquota option set on /home partition (Automated)	85
Journal filesystems.....	87
Setting quotas	87
Reporting	87
1.1.7.5 Ensure grpquota option set on /home partition (Automated)	88
Journal filesystems.....	90
Setting quotas	90
Reporting	90
1.1.8 Configure /dev/shm.....	91
1.1.8.1 Ensure nodev option set on /dev/shm partition (Automated)	92
1.1.8.2 Ensure noexec option set on /dev/shm partition (Automated)	94
1.1.8.3 Ensure nosuid option set on /dev/shm partition (Automated)	96
1.1.9 Disable Automounting (Automated)	98
1.1.10 Disable USB Storage (Automated)	100

1.2 Configure Software Updates	102
1.2.1 Ensure package manager repositories are configured (Manual).....	103
1.2.2 Ensure GPG keys are configured (Manual)	105
1.3 Filesystem Integrity Checking	107
1.3.1 Ensure AIDE is installed (Automated)	108
1.3.2 Ensure filesystem integrity is regularly checked (Automated)	110
1.4 Secure Boot Settings.....	113
1.4.1 Ensure bootloader password is set (Automated)	114
1.4.2 Ensure permissions on bootloader config are configured (Automated).....	117
1.4.3 Ensure authentication required for single user mode (Automated)	119
1.5 Additional Process Hardening	120
1.5.1 Ensure XD/NX support is enabled (Manual)	121
1.5.2 Ensure address space layout randomization (ASLR) is enabled (Automated).....	123
1.5.3 Ensure prelink is not installed (Automated).....	126
1.5.4 Ensure core dumps are restricted (Automated)	128
1.6 Mandatory Access Control	130
1.6.1 Configure AppArmor.....	131
1.6.1.1 Ensure AppArmor is installed (Automated)	132
1.6.1.2 Ensure AppArmor is enabled in the bootloader configuration (Automated).....	134
1.6.1.3 Ensure all AppArmor Profiles are in enforce or complain mode (Automated)	136
1.6.1.4 Ensure all AppArmor Profiles are enforcing (Automated).....	138
1.7 Command Line Warning Banners	140
1.7.1 Ensure message of the day is configured properly (Automated).....	141
1.7.2 Ensure local login warning banner is configured properly (Automated)	143
1.7.3 Ensure remote login warning banner is configured properly (Automated).....	145
1.7.4 Ensure permissions on /etc/motd are configured (Automated)	147
1.7.5 Ensure permissions on /etc/issue are configured (Automated)	149
1.7.6 Ensure permissions on /etc/issue.net are configured (Automated)	151
1.8 GNOME Display Manager.....	153
1.8.1 Ensure GNOME Display Manager is removed (Automated)	154
1.8.2 Ensure GDM login banner is configured (Automated)	156
1.8.3 Ensure disable-user-list option is enabled (Automated)	161
1.8.4 Ensure GDM screen locks when the user is idle (Automated)	165
1.8.5 Ensure GDM screen locks cannot be overridden (Automated)	170
1.8.6 Ensure automatic mounting of removable media is disabled (Automated).....	175
1.8.7 Ensure XDCMP is not enabled (Automated)	177
1.9 Ensure updates, patches, and additional security software are installed (Manual)	179
2 Services.....	181
2.1 Configure Time Synchronization	182
2.1.1 Ensure time synchronization is in use.....	183
2.1.1.1 Ensure a single time synchronization daemon is in use (Automated)	184
2.1.2 Configure chrony	188
2.1.2.1 Ensure chrony is configured with authorized timeserver (Manual)	189
2.1.2.2 Ensure chrony is running as user _chrony (Automated)	193
2.1.2.3 Ensure chrony is enabled and running (Automated)	195
2.1.3 Configure systemd-timesyncd.....	197
2.1.3.1 Ensure systemd-timesyncd configured with authorized timeserver (Manual).....	199
2.1.3.2 Ensure systemd-timesyncd is enabled and running (Automated)	203
2.1.4 Configure ntp	205
2.1.4.1 Ensure ntp access control is configured (Automated)	206
2.1.4.2 Ensure ntp is configured with authorized timeserver (Manual)	210

2.1.4.3 Ensure ntp is running as user ntp (Automated).....	213
2.1.4.4 Ensure ntp is enabled and running (Automated).....	215
2.2 Special Purpose Services	217
2.2.1 Ensure X Window System is not installed (Automated)	218
2.2.2 Ensure Avahi Server is not installed (Automated).....	220
2.2.3 Ensure CUPS is not installed (Automated)	222
2.2.4 Ensure DHCP Server is not installed (Automated).....	224
2.2.5 Ensure LDAP server is not installed (Automated).....	226
2.2.6 Ensure NFS is not installed (Automated)	228
2.2.7 Ensure DNS Server is not installed (Automated)	229
2.2.8 Ensure FTP Server is not installed (Automated)	231
2.2.9 Ensure HTTP server is not installed (Automated)	233
2.2.10 Ensure IMAP and POP3 server are not installed (Automated).....	235
2.2.11 Ensure Samba is not installed (Automated)	237
2.2.12 Ensure HTTP Proxy Server is not installed (Automated)	239
2.2.13 Ensure SNMP Server is not installed (Automated)	241
2.2.14 Ensure NIS Server is not installed (Automated).....	243
2.2.15 Ensure mail transfer agent is configured for local-only mode (Automated).....	245
2.2.16 Ensure rsync service is either not installed or masked (Automated).....	247
2.3 Service Clients	249
2.3.1 Ensure NIS Client is not installed (Automated)	250
2.3.2 Ensure rsh client is not installed (Automated)	252
2.3.3 Ensure talk client is not installed (Automated)	254
2.3.4 Ensure telnet client is not installed (Automated)	256
2.3.5 Ensure LDAP client is not installed (Automated).....	258
2.3.6 Ensure RPC is not installed (Automated)	260
2.4 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 Ensure system is checked to determine if IPv6 is enabled (Manual)	266
3.1.2 Ensure wireless interfaces are disabled (Automated)	270
3.2 Network Parameters (Host Only).....	273
3.2.1 Ensure packet redirect sending is disabled (Automated)	274
3.2.2 Ensure IP forwarding is disabled (Automated)	278
3.3 Network Parameters (Host and Router).....	282
3.3.1 Ensure source routed packets are not accepted (Automated)	283
3.3.2 Ensure ICMP redirects are not accepted (Automated).....	287
3.3.3 Ensure secure ICMP redirects are not accepted (Automated)	291
3.3.4 Ensure suspicious packets are logged (Automated)	295
3.3.5 Ensure broadcast ICMP requests are ignored (Automated).....	299
3.3.6 Ensure bogus ICMP responses are ignored (Automated).....	302
3.3.7 Ensure Reverse Path Filtering is enabled (Automated)	305
3.3.8 Ensure TCP SYN Cookies is enabled (Automated)	309
3.3.9 Ensure IPv6 router advertisements are not accepted (Automated).....	312
3.4 Uncommon Network Protocols	316
3.4.1 Ensure DCCP is disabled (Automated)	317
3.4.2 Ensure SCTP is disabled (Automated).....	319
3.4.3 Ensure RDS is disabled (Automated)	321
3.4.4 Ensure TIPC is disabled (Automated)	323
3.5 Firewall Configuration	325
3.5.1 Configure UncomplicatedFirewall	326

3.5.1.1 Ensure ufw is installed (Automated).....	327
3.5.1.2 Ensure iptables-persistent is not installed with ufw (Automated)	329
3.5.1.3 Ensure ufw service is enabled (Automated).....	331
3.5.1.4 Ensure ufw loopback traffic is configured (Automated)	334
3.5.1.5 Ensure ufw outbound connections are configured (Manual)	336
3.5.1.6 Ensure ufw firewall rules exist for all open ports (Automated).....	338
3.5.1.7 Ensure ufw default deny firewall policy (Automated).....	340
3.5.2 Configure nftables.....	342
3.5.2.1 Ensure nftables is installed (Automated).....	345
3.5.2.2 Ensure ufw is uninstalled or disabled with nftables (Automated)	347
3.5.2.3 Ensure iptables are flushed with nftables (Manual).....	349
3.5.2.4 Ensure a nftables table exists (Automated).....	351
3.5.2.5 Ensure nftables base chains exist (Automated)	353
3.5.2.6 Ensure nftables loopback traffic is configured (Automated)	355
3.5.2.7 Ensure nftables outbound and established connections are configured (Manual)	357
3.5.2.8 Ensure nftables default deny firewall policy (Automated).....	359
3.5.2.9 Ensure nftables service is enabled (Automated).....	361
3.5.2.10 Ensure nftables rules are permanent (Automated).....	362
3.5.3 Configure iptables.....	365
3.5.3.1 Configure iptables software	366
3.5.3.1.1 Ensure iptables packages are installed (Automated)	367
3.5.3.1.2 Ensure nftables is not installed with iptables (Automated)	369
3.5.3.1.3 Ensure ufw is uninstalled or disabled with iptables (Automated).....	370
3.5.3.2 Configure IPv4 iptables.....	372
3.5.3.2.1 Ensure iptables default deny firewall policy (Automated)	373
3.5.3.2.2 Ensure iptables loopback traffic is configured (Automated)	375
3.5.3.2.3 Ensure iptables outbound and established connections are configured (Manual)	377
3.5.3.2.4 Ensure iptables firewall rules exist for all open ports (Automated)	379
3.5.3.3 Configure IPv6 ip6tables.....	382
3.5.3.3.1 Ensure ip6tables default deny firewall policy (Automated)	383
3.5.3.3.2 Ensure ip6tables loopback traffic is configured (Automated)	386
3.5.3.3.3 Ensure ip6tables outbound and established connections are configured (Manual)	389
3.5.3.3.4 Ensure ip6tables firewall rules exist for all open ports (Automated)	392
4 Logging and Auditing.....	395
4.1 Configure Logging.....	396
Security principals for logging	396
What is covered	396
What is not covered.....	396
4.1.1 Configure journald	397
4.1.1.1 Ensure journald is configured to send logs to a remote log host.....	398
4.1.1.1.1 Ensure systemd-journal-remote is installed (Manual)	399
4.1.1.1.2 Ensure systemd-journal-remote is configured (Manual).....	401
4.1.1.1.3 Ensure systemd-journal-remote is enabled (Manual).....	403
4.1.1.1.4 Ensure journald is not configured to receive logs from a remote client (Automated)	405
4.1.1.2 Ensure journald service is enabled (Automated).....	407
4.1.1.3 Ensure journald is configured to compress large log files (Automated).....	409
4.1.1.4 Ensure journald is configured to write logfiles to persistent disk (Automated).....	411
4.1.1.5 Ensure journald is not configured to send logs to rsyslog (Manual)	413
4.1.1.6 Ensure journald log rotation is configured per site policy (Manual)	415
4.1.1.7 Ensure journald default file permissions configured (Manual)	417
4.1.2 Configure rsyslog.....	419
4.1.2.1 Ensure rsyslog is installed (Automated)	420

4.1.2.2 Ensure rsyslog service is enabled (Automated)	422
4.1.2.3 Ensure journald is configured to send logs to rsyslog (Manual)	424
4.1.2.4 Ensure rsyslog default file permissions are configured (Automated)	426
4.1.2.5 Ensure logging is configured (Manual).....	428
4.1.2.6 Ensure rsyslog is configured to send logs to a remote log host (Manual)	431
Old format	431
New format.....	431
4.1.2.7 Ensure rsyslog is not configured to receive logs from a remote client (Automated)	433
Old format	433
New format.....	433
Old format	434
New format.....	434
4.1.3 Ensure all logfiles have appropriate permissions and ownership (Automated)	436
4.2 Configure System Accounting (auditd).....	441
Normalization.....	442
Capacity planning	442
4.2.1 Ensure auditing is enabled	443
4.2.1.1 Ensure auditd is installed (Automated).....	444
4.2.1.2 Ensure auditd service is enabled and active (Automated)	446
4.2.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated)	448
4.2.1.4 Ensure audit_backlog_limit is sufficient (Automated)	450
4.2.2 Configure Data Retention.....	452
4.2.2.1 Ensure audit log storage size is configured (Automated).....	453
4.2.2.2 Ensure audit logs are not automatically deleted (Automated)	455
4.2.2.3 Ensure system is disabled when audit logs are full (Automated)	457
4.2.3 Configure auditd rules	459
4.2.3.1 Ensure changes to system administration scope (sudoers) is collected (Automated).....	460
On disk configuration	461
Running configuration.....	461
Potential reboot required.....	462
System call structure	462
4.2.3.2 Ensure actions as another user are always logged (Automated)	464
64 Bit systems	465
32 Bit systems	465
Create audit rules	466
64 Bit systems.....	466
Load audit rules.....	466
32 Bit systems.....	466
Potential reboot required.....	466
System call structure	466
4.2.3.3 Ensure events that modify the sudo log file are collected (Automated).....	468
On disk configuration	469
Running configuration.....	469
Potential reboot required.....	470
System call structure	470
4.2.3.4 Ensure events that modify date and time information are collected (Automated)	471
64 Bit systems	471
32 Bit systems	472
Create audit rules	473
64 Bit systems.....	473
Load audit rules.....	473
32 Bit systems.....	473
Potential reboot required.....	474

System call structure	474
4.2.3.5 Ensure events that modify the system's network environment are collected (Automated)	475
64 Bit systems	475
32 Bit systems	476
Create audit rules	477
64 Bit systems.....	477
Load audit rules.....	477
32 Bit systems.....	477
Potential reboot required.....	477
System call structure	477
4.2.3.6 Ensure use of privileged commands are collected (Automated)	479
On disk configuration	480
Running configuration.....	480
Special mount points	480
Special mount points	481
Potential reboot required.....	482
System call structure	482
4.2.3.7 Ensure unsuccessful file access attempts are collected (Automated)	483
64 Bit systems	483
32 Bit systems	484
Create audit rules	485
64 Bit systems.....	485
Load audit rules.....	485
32 Bit systems.....	485
Potential reboot required.....	486
System call structure	486
4.2.3.8 Ensure events that modify user/group information are collected (Automated)	487
On disk configuration	488
Running configuration.....	488
Potential reboot required.....	489
System call structure	489
4.2.3.9 Ensure discretionary access control permission modification events are collected (Automated)	491
64 Bit systems	492
32 Bit systems	493
Create audit rules	494
64 Bit systems.....	494
Load audit rules.....	494
32 Bit systems.....	494
Potential reboot required.....	495
System call structure	495
4.2.3.10 Ensure successful file system mounts are collected (Automated)	496
64 Bit systems	497
32 Bit systems	497
Create audit rules	498
64 Bit systems.....	498
Load audit rules.....	498
32 Bit systems.....	498
Potential reboot required.....	498
System call structure	498
4.2.3.11 Ensure session initiation information is collected (Automated)	500
On disk configuration	501
Running configuration.....	501
Potential reboot required.....	502
System call structure	502

4.2.3.12 Ensure login and logout events are collected (Automated)	504
On disk configuration	505
Running configuration.....	505
Potential reboot required.....	506
System call structure	506
4.2.3.13 Ensure file deletion events by users are collected (Automated).....	508
64 Bit systems	509
32 Bit systems	509
Create audit rules	510
64 Bit systems.....	510
Load audit rules.....	510
32 Bit systems.....	510
Potential reboot required.....	510
System call structure	510
4.2.3.14 Ensure events that modify the system's Mandatory Access Controls are collected (Automated).....	512
On disk configuration	513
Running configuration.....	513
Potential reboot required.....	514
System call structure	514
4.2.3.15 Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)	516
64 Bit systems	517
32 Bit systems	517
Create audit rules	518
64 Bit systems.....	518
Load audit rules.....	518
32 Bit systems.....	518
Potential reboot required.....	518
System call structure	518
4.2.3.16 Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated)	520
64 Bit systems	521
32 Bit systems	521
Create audit rules	522
64 Bit systems.....	522
Load audit rules.....	522
32 Bit systems.....	522
Potential reboot required.....	522
System call structure	522
4.2.3.17 Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)	524
64 Bit systems	525
32 Bit systems	525
Create audit rules	526
64 Bit systems.....	526
Load audit rules.....	526
32 Bit systems.....	526
Potential reboot required.....	526
System call structure	526
4.2.3.18 Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)	528
64 Bit systems	529
32 Bit systems	529
Create audit rules	530
64 Bit systems.....	530

Load audit rules	530
32 Bit systems	530
Potential reboot required	530
System call structure	530
4.2.3.19 Ensure kernel module loading unloading and modification is collected (Automated)	532
64 Bit systems	533
Symlink audit	534
Create audit rules	535
64 Bit systems	535
Load audit rules	535
Potential reboot required	535
System call structure	535
4.2.3.20 Ensure the audit configuration is immutable (Automated)	537
4.2.3.21 Ensure the running and on disk configuration is the same (Manual)	539
Merged rule sets	539
Potential reboot required	540
4.2.4 Configure auditd file access	541
4.2.4.1 Ensure audit log files are mode 0600 or less permissive (Automated)	542
4.2.4.2 Ensure only authorized users own audit log files (Automated)	544
4.2.4.3 Ensure only authorized groups are assigned ownership of audit log files (Automated)	546
4.2.4.4 Ensure the audit log directory is 0750 or more restrictive (Automated)	548
4.2.4.5 Ensure audit configuration files are 640 or more restrictive (Automated)	550
4.2.4.6 Ensure audit configuration files are owned by root (Automated)	552
4.2.4.7 Ensure audit configuration files belong to group root (Automated)	554
4.2.4.8 Ensure audit tools are 755 or more restrictive (Automated)	556
4.2.4.9 Ensure audit tools are owned by root (Automated)	558
4.2.4.10 Ensure audit tools belong to group root (Automated)	560
4.2.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)	562
5 Access, Authentication and Authorization	564
5.1 Configure time-based job schedulers	565
5.1.1 Ensure cron daemon is enabled and running (Automated)	566
5.1.2 Ensure permissions on /etc/crontab are configured (Automated)	568
5.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)	570
5.1.4 Ensure permissions on /etc/cron.daily are configured (Automated)	572
5.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated)	574
5.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated)	576
5.1.7 Ensure permissions on /etc/cron.d are configured (Automated)	578
5.1.8 Ensure cron is restricted to authorized users (Automated)	580
5.1.9 Ensure at is restricted to authorized users (Automated)	582
5.2 Configure SSH Server	584
5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	585
5.2.2 Ensure permissions on SSH private host key files are configured (Automated)	587
5.2.3 Ensure permissions on SSH public host key files are configured (Automated)	591
5.2.4 Ensure SSH access is limited (Automated)	594
5.2.5 Ensure SSH LogLevel is appropriate (Automated)	597
5.2.6 Ensure SSH PAM is enabled (Automated)	599
5.2.7 Ensure SSH root login is disabled (Automated)	601
5.2.8 Ensure SSH HostbasedAuthentication is disabled (Automated)	603
5.2.9 Ensure SSH PermitEmptyPasswords is disabled (Automated)	605
5.2.10 Ensure SSH PermitUserEnvironment is disabled (Automated)	607
5.2.11 Ensure SSH IgnoreRhosts is enabled (Automated)	609
5.2.12 Ensure SSH X11 forwarding is disabled (Automated)	611

5.2.13 Ensure only strong Ciphers are used (Automated)	613
5.2.14 Ensure only strong MAC algorithms are used (Automated)	616
5.2.15 Ensure only strong Key Exchange algorithms are used (Automated)	619
5.2.16 Ensure SSH AllowTcpForwarding is disabled (Automated)	622
5.2.17 Ensure system-wide crypto policy is not over-ridden (Automated).....	624
5.2.18 Ensure SSH warning banner is configured (Automated).....	626
5.2.19 Ensure SSH MaxAuthTries is set to 4 or less (Automated).....	628
5.2.20 Ensure SSH MaxStartups is configured (Automated)	630
5.2.21 Ensure SSH MaxSessions is set to 10 or less (Automated).....	632
5.2.22 Ensure SSH LoginGraceTime is set to one minute or less (Automated).....	634
5.2.23 Ensure SSH Idle Timeout Interval is configured (Automated)	636
5.3 Configure privilege escalation	639
sudo	639
pkexec	639
5.3.1 Ensure sudo is installed (Automated)	640
5.3.2 Ensure sudo commands use pty (Automated)	642
5.3.3 Ensure sudo log file exists (Automated).....	644
5.3.4 Ensure users must provide password for privilege escalation (Automated)	646
5.3.5 Ensure re-authentication for privilege escalation is not disabled globally (Automated)	648
5.3.6 Ensure sudo authentication timeout is configured correctly (Automated).....	650
5.3.7 Ensure access to the su command is restricted (Automated)	652
5.4 Configure PAM	654
5.4.1 Ensure password creation requirements are configured (Automated)	655
Password length.....	656
Password complexity.....	656
5.4.2 Ensure lockout for failed password attempts is configured (Automated).....	659
Common auth	660
Common account	660
Fail lock configuration	660
Common auth	661
Common account	661
Fail lock configuration	661
5.4.3 Ensure password reuse is limited (Automated).....	663
5.4.4 Ensure password hashing algorithm is up to date with the latest standards (Automated)	665
PAM.....	666
Login definitions	666
PAM.....	666
Login definitions	666
5.4.5 Ensure all current passwords uses the configured hashing algorithm (Manual)	668
5.5 User Accounts and Environment	670
5.5.1 Set Shadow Password Suite Parameters	671
5.5.1.1 Ensure minimum days between password changes is configured (Automated)	672
5.5.1.2 Ensure password expiration is 365 days or less (Automated).....	674
5.5.1.3 Ensure password expiration warning days is 7 or more (Automated)	676
5.5.1.4 Ensure inactive password lock is 30 days or less (Automated).....	678
5.5.1.5 Ensure all users last password change date is in the past (Automated)	680
5.5.2 Ensure system accounts are secured (Automated)	682
5.5.3 Ensure default group for the root account is GID 0 (Automated)	684
5.5.4 Ensure default user umask is 027 or more restrictive (Automated).....	686
5.5.5 Ensure default user shell timeout is 900 seconds or less (Automated)	691
6 System Maintenance	695
6.1 System File Permissions	696

6.1.1 Ensure permissions on /etc/passwd are configured (Automated)	697
6.1.2 Ensure permissions on /etc/passwd- are configured (Automated)	699
6.1.3 Ensure permissions on /etc/group are configured (Automated)	701
6.1.4 Ensure permissions on /etc/group- are configured (Automated)	703
6.1.5 Ensure permissions on /etc/shadow are configured (Automated)	705
6.1.6 Ensure permissions on /etc/shadow- are configured (Automated)	707
6.1.7 Ensure permissions on /etc/gshadow are configured (Automated)	709
6.1.8 Ensure permissions on /etc/gshadow- are configured (Automated)	711
6.1.9 Ensure no world writable files exist (Automated)	713
6.1.10 Ensure no unowned files or directories exist (Automated)	715
6.1.11 Ensure no ungrouped files or directories exist (Automated)	717
6.1.12 Audit SUID executables (Manual)	719
6.1.13 Audit SGID executables (Manual)	721
6.2 Local User and Group Settings	723
6.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated)	724
6.2.2 Ensure /etc/shadow password fields are not empty (Automated)	726
6.2.3 Ensure all groups in /etc/passwd exist in /etc/group (Automated)	728
6.2.4 Ensure shadow group is empty (Automated)	730
6.2.5 Ensure no duplicate UIDs exist (Automated)	732
6.2.6 Ensure no duplicate GIDs exist (Automated)	734
6.2.7 Ensure no duplicate user names exist (Automated)	736
6.2.8 Ensure no duplicate group names exist (Automated)	738
6.2.9 Ensure root PATH Integrity (Automated)	740
6.2.10 Ensure root is the only UID 0 account (Automated)	742
6.2.11 Ensure local interactive user home directories exist (Automated)	744
6.2.12 Ensure local interactive users own their home directories (Automated)	746
6.2.13 Ensure local interactive user home directories are mode 750 or more restrictive (Automated)	748
6.2.14 Ensure no local interactive user has .netrc files (Automated)	751
6.2.15 Ensure no local interactive user has .forward files (Automated)	754
6.2.16 Ensure no local interactive user has .rhosts files (Automated)	756
6.2.17 Ensure local interactive user dot files are not group or world writable (Automated)	758
Appendix: Summary Table	762
Appendix: Change History	782

Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document provides prescriptive guidance for establishing a secure configuration posture for Ubuntu Linux 22.04 LTS systems running on x64 platforms.

Many lists are included including filesystem types, services, clients, and network protocols. Not all items in these lists are guaranteed to exist on all distributions and additional similar items may exist which should be considered in addition to those explicitly mentioned.

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 a Ubuntu Linux 22.04 LTS system running on x64 platforms

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. 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/>.

DRAFT

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

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

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

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) '4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

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.

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
Graham Eames
Alexander Scheel
Martinus Nel

Editor

Jonathan Lewis Christopherson
Eric Pinnell
Justin Brown

Recommendations

DRAFT

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.

DRAFT

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. For the current available file system modules on the system see `/usr/lib/modules/$(uname -r)/kernel/fs`

Start up scripts

Kernel modules loaded directly via `insmod` will ignore what is configured in the relevant `/etc/modprobe.d/*.conf` files. If modules are still being loaded after a reboot whilst having the correctly configured `blacklist` and `install` command, check for `insmod` entries in start up scripts such as `.bashrc`.

You may also want to check `/usr/lib/modprobe.d/`. Please note that this directory should not be used for user defined module loading. Ensure that all such entries resides in `/etc/modprobe.d/*.conf` files.

Return values

By using `/bin/false` as the command in disabling a particular module service two purposes; to convey the meaning of the entry to the user and cause a non-zero return value. The latter can be tested for in scripts. Please note that `insmod` will ignore what is configured in the relevant `/etc/modprobe.d/*.conf` files. The preferred way to load modules is with `modprobe`.

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 system. If this filesystem type is not needed, disable it.

Audit:

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

- How will the module be loaded.

```
# modprobe -n -v cramfs | grep "^install"
install /bin/false
```

- Is the module currently loaded.

```
# lsmod | grep cramfs
<No output>
```

- Is the module blacklisted.

```
# grep -E "^blacklist\s+cramfs" /etc/modprobe.d/*
blacklist      cramfs
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf` with a line that reads `install cramfs /bin/false` and a line that reads `blacklist cramfs`.

Example:

```
# printf "install cramfs /bin/false  
blacklist cramfs  
" >> /etc/modprobe.d/cramfs.conf
```

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

```
# modprobe -r cramfs
```

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0005	M1050

1.1.1.2 Ensure mounting of squashfs filesystems is disabled (Automated)

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. 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:

As Snap packages utilize `squashfs` as a compressed filesystem, disabling `squashfs` will cause Snap packages to fail.

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.

Audit:

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

- How will the module be loaded.

```
# modprobe -n -v squashfs | grep "^install"  
install /bin/false
```

- Is the module currently loaded.

```
# lsmod | grep squashfs  
<No output>
```

- Is the module blacklisted.

```
# grep -E "^blacklist\s+squashfs" /etc/modprobe.d/*  
/etc/modprobe.d/squashfs.conf:blacklist      squashfs
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf` with the lines that reads `install squashfs /bin/false` and `blacklist squashfs`.

Example:

```
# printf "install squashfs /bin/false  
blacklist squashfs  
" >> /etc/modprobe.d/squashfs.conf
```

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

```
# modprobe -r squashfs
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</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 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0005	M1050

1.1.1.3 Ensure mounting of udf filesystems is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - 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.

Impact:

Microsoft Azure requires the usage of `udf`.

`udf` should not be disabled on systems run on Microsoft Azure.

Audit:

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

- How will the module be loaded.

```
# modprobe -n -v udf | grep "^install"
install /bin/false
```

- Is the module currently loaded.

```
# lsmod | grep udf
<No output>
```

- Is the module blacklisted.

```
# grep -E "^blacklist[:blank:]*udf" /etc/modprobe.d/*
/etc/modprobe.d/udf.conf:blacklist      udf
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf` with a line that reads `install udf /bin/false`.

Example:

```
# printf "install udf /bin/false
blacklist udf
" >> /etc/modprobe.d/udf.conf
```

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

```
# modprobe -r udf
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0005	M1050

1.1.2 Configure /tmp

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

DRAFT

1.1.2.1 Ensure /tmp is a separate partition (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 additional mount options such as 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 hard link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard link 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 configuration where `/tmp` is not a separate file system it will essentially have the whole disk available, as the default installation 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. Another alternative is to create a dedicated partition for `/tmp` from a separate volume or disk. One of the downsides of a disk-based dedicated partition is that it will be slower than `tmpfs` which is RAM-based.

`/tmp` utilizing `tmpfs` can be resized using the `size={size}` parameter in the relevant entry in `/etc/fstab`.

Audit:

Run the following command and verify the output shows that `/tmp` is mounted. Particular requirements pertaining to mount options are covered in ensuing sections.

```
# findmnt --kernel /tmp
TARGET SOURCE FSTYPE OPTIONS
/tmp tmpfs tmpfs rw,nosuid,nodev,noexec,inode6
```

Ensure that systemd will mount the `/tmp` partition at boot time.

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

Note that by default systemd will output generated if there is an entry in `/etc/fstab` for `/tmp`. This just means systemd will use the entry in `/etc/fstab` instead of its default unit file configuration for `/tmp`.

Remediation:

First ensure that systemd is correctly configured to ensure that `/tmp` will be mounted at boot time.

```
# systemctl unmask tmp.mount
```

For specific configuration requirements of the `/tmp` mount for your environment, modify `/etc/fstab` or `tmp.mount`.

Example of `/etc/fstab` configured `tmpfs` file system with specific mount options:

```
tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime,size=2G 0
```

Example of `tmp.mount` configured `tmpfs` file system with specific mount options:

```
[Unit]
Description=Temporary Directory /tmp
ConditionPathIsSymbolicLink=!/tmp
DefaultDependencies=no
Conflicts=umount.target
Before=local-fs.target umount.target
After=swap.target

[Mount]
What=tmpfs
Where=/tmp
Type=tmpfs
```

References:

1. <https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/>
2. <https://www.freedesktop.org/software/systemd/man/systemd-fstab-generator.html>

Additional Information:

If an entry for `/tmp` exists in `/etc/fstab` it will take precedence over entries in systemd unit file.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.1 Associate Active Ports, Services and Protocols to Asset Inventory</u></p> <p>Associate active ports, services and protocols to the hardware assets in the asset inventory.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1022

1.1.2.2 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 create a block or character special devices in `/tmp`.

Audit:

Verify that the `nodev` option is set for the `/tmp` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /tmp | grep nodev  
  
/tmp  tmpfs  tmpfs  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/tmp` partition.

Example:

```
<device> /tmp      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/tmp` with the configured options:

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

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1022

1.1.2.3 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:

Verify that the `noexec` option is set for the `/tmp` mount.

Run the following command to verify that the `noexec` mount option is set.

Example:

```
# findmnt --kernel /tmp | grep noexec  
/tmp    tmpfs    tmpfs    rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/tmp` partition.

Example:

```
<device> /tmp    <fstype>    defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/tmp` with the configured options:

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

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0005	M1022

1.1.2.4 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:

Verify that the `nosuid` option is set for the `/tmp` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /tmp | grep nosuid  
/tmp  tmpfs  tmpfs  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/tmp` partition.

Example:

```
<device> /tmp      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/tmp` with the configured options:

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

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1022

1.1.3 Configure /var

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.

DRAFT

1.1.3.1 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:

The reasoning for mounting `/var` on a separate partition is as follow.

Protection from resource exhaustion

The default installation only creates a single `/` partition. Since the `/var` directory may contain world-writable files and directories, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/var` and cause unintended behavior across the system as the disk is full. See `man auditd.conf` for details.

Fine grained control over the mount

Configuring `/var` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limits an attackers ability to create exploits on the system. Other options allow for specific behaviour. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

Protection from exploitation

An example of exploiting `/var` may be an attacker establishing a hard-link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard-link 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` is mounted.

Example:

```
# findmnt --kernel /var  
  
TARGET SOURCE FSType OPTIONS  
/var /dev/sdb ext4 rw,relatime,seclabel,data=ordered
```

Remediation:

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

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

References:

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

Additional Information:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0006	

1.1.3.2 Ensure nodev option set on /var 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 `/var` filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in `/var`.

Audit:

Verify that the `nodev` option is set for the `/var` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /var | grep nodev  
/var    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var` partition.

Example:

```
<device> /var      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var` with the configured options:

```
# mount -o remount /var
```

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1038

1.1.3.3 Ensure noexec option set on /var 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 `/var` filesystem is only intended for variable files such as logs, set this option to ensure that users cannot run executable binaries from `/var`.

Audit:

Verify that the `noexec` option is set for the `/var` mount.

Run the following command to verify that the `noexec` mount option is set.

Example:

```
# findmnt --kernel /var | grep noexec  
/var    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var` partition.

Example:

```
<device> /var    <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var` with the configured options:

```
# mount -o remount /var
```

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0005	M1022

1.1.3.4 Ensure nosuid option set on /var 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 `/var` filesystem is only intended for variable files such as logs, set this option to ensure that users cannot create `setuid` files in `/var`.

Audit:

Verify that the `nosuid` option is set for the `/var` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /var | grep nosuid  
/var    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var` partition.

Example:

```
<device> /var      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var` with the configured options:

```
# mount -o remount /var
```

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1038

1.1.4 Configure /var/tmp

The `/var/tmp` directory is a world-writable directory used for temporary storage by all users and some applications. Temporary file residing in `/var/tmp` is to be preserved between reboots.

DRAFT

1.1.4.1 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. Temporary file residing in `/var/tmp` is to be preserved between reboots.

Rationale:

The reasoning for mounting `/var/tmp` on a separate partition is as follow.

Protection from resource exhaustion

The default installation only creates a single `/` partition. Since the `/var/tmp` directory may contain world-writable files and directories, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/var/tmp` and cause the potential disruption to daemons as the disk is full.

Fine grained control over the mount

Configuring `/var/tmp` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limits an attackers ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

Protection from exploitation

An example of exploiting `/var/tmp` may be an attacker establishing a hard-link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard-link 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.
Example:

```
# findmnt --kernel /var/tmp  
  
TARGET SOURCE FSTYPE OPTIONS  
/var/tmp /dev/sdb ext4 rw,relatime,seclabel,data=ordered
```

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.

References:

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

Additional Information:

When modifying `/var/tmp` 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 multi-user mode.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1022

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

Audit:

Verify that the `noexec` option is set for the `/var/tmp` mount.

Run the following command to verify that the `noexec` mount option is set.

Example:

```
# findmnt --kernel /var/tmp | grep noexec
/var/tmp  /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var/tmp` partition.

Example:

```
<device> /var/tmp      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/var/tmp` with the configured options:

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

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0005	M1022

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

Audit:

Verify that the `nosuid` option is set for the `/var/tmp` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /var/tmp | grep nosuid  
  
/var/tmp    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var/tmp` partition.

Example:

```
<device> /var/tmp      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
```

Run the following command to remount `/var/tmp` with the configured options:

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

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1022

1.1.4.4 Ensure nodev option set on /var/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 `/var/tmp` filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in `/var/tmp`.

Audit:

Verify that the `nodev` option is set for the `/var/tmp` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /var/tmp | grep nodev  
/var/tmp    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var/tmp` partition.

Example:

```
<device> /var/tmp      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
```

Run the following command to remount `/var/tmp` with the configured options:

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

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1022

1.1.5 Configure /var/log

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

DRAFT

1.1.5.1 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:

The reasoning for mounting `/var/log` on a separate partition is as follow.

Protection from resource exhaustion

The default installation only creates a single `/` partition. Since the `/var/log` directory contain the log files that can grow quite large, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole.

Fine grained control over the mount

Configuring `/var/log` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limits an attackers ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

Protection of log data

As `/var/log` contains log files, care should be taken to ensure the security and integrity of the data and mount point.

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 --kernel /var/log  
  
TARGET      SOURCE   FSTYPE OPTIONS  
/var/log    /dev/sdb ext4    rw,relatime,seclabel,data=ordered
```

Remediation:

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

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

References:

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

Additional Information:

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

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1022

1.1.5.2 Ensure nodev option set on /var/log 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 `/var/log` filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in `/var/log`.

Audit:

Verify that the `nodev` option is set for the `/var/log` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /var/log | grep nodev  
/var/log  /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var/log` partition.

Example:

```
<device> /var/log      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
```

Run the following command to remount `/var/log` with the configured options:

```
# mount -o remount /var/log
```

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1022

1.1.5.3 Ensure noexec option set on /var/log 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 `/var/log` filesystem is only intended for log files, set this option to ensure that users cannot run executable binaries from `/var/log`.

Audit:

Verify that the `noexec` option is set for the `/var/log` mount.

Run the following command to verify that the `noexec` mount option is set.

Example:

```
# findmnt --kernel /var/log | grep noexec  
/var/log    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var/log` partition.

Example:

```
<device> /var/log      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0  
0
```

Run the following command to remount `/var/log` with the configured options:

```
# mount -o remount /var/log
```

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0005	M1022

1.1.5.4 Ensure nosuid option set on /var/log 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 `/var/log` filesystem is only intended for log files, set this option to ensure that users cannot create `setuid` files in `/var/log`.

Audit:

Verify that the `nosuid` option is set for the `/var/log` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /var/log | grep nosuid  
/var/log  /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var/log` partition.

Example:

```
<device> /var/log      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
```

Run the following command to remount `/var/log` with the configured options:

```
# mount -o remount /var/log
```

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1022

1.1.6 Configure /var/log/audit

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

DRAFT

1.1.6.1 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:

The reasoning for mounting `/var/log/audit` on a separate partition is as follow.

Protection from resource exhaustion

The default installation only creates a single `/` partition. Since the `/var/log/audit` directory contains the `audit.log` file that can grow quite large, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/var/log/audit` and cause `auditd` to trigger its `space_left_action` as the disk is full. See `man auditd.conf` for details.

Fine grained control over the mount

Configuring `/var/log/audit` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limit an attacker's ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

Protection of audit data

As `/var/log/audit` contains audit logs, care should be taken to ensure the security and integrity of the data and mount point.

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 --kernel /var/log/audit  
  
TARGET      SOURCE   FSTYPE OPTIONS  
/var/log/audit /dev/sdb ext4    rw,relatime,seclabel,data=ordered
```

Remediation:

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

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

References:

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

Additional Information:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1022

1.1.6.2 Ensure noexec option set on /var/log/audit 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 `/var/log/audit` filesystem is only intended for audit logs, set this option to ensure that users cannot run executable binaries from `/var/log/audit`.

Audit:

Verify that the `noexec` option is set for the `/var/log/audit` mount.

Run the following command to verify that the `noexec` mount option is set.

Example:

```
# findmnt --kernel /var/log/audit | grep noexec
/var/log/audit  /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var` partition.

Example:

```
<device> /var/log/audit    <fstype>
defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var/log/audit` with the configured options:

```
# mount -o remount /var/log/audit
```

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0005	M1022

1.1.6.3 Ensure nodev option set on /var/log/audit 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 `/var/log/audit` filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in `/var/log/audit`.

Audit:

Verify that the `nodev` option is set for the `/var/log/audit` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /var/log/audit | grep nodev
/var/log/audit  /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var/log/audit` partition.

Example:

```
<device> /var/log/audit    <fstype>
defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var/log/audit` with the configured options:

```
# mount -o remount /var/log/audit
```

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1022

1.1.6.4 Ensure nosuid option set on /var/log/audit 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 `/var/log/audit` filesystem is only intended for variable files such as logs, set this option to ensure that users cannot create `setuid` files in `/var/log/audit`.

Audit:

Verify that the `nosuid` option is set for the `/var/log/audit` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /var/log/audit | grep nosuid
/var/log/audit  /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var/log/audit` partition.

Example:

```
<device> /var/log/audit    <fstype>
defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var/log/audit` with the configured options:

```
# mount -o remount /var/log/audit
```

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1022

1.1.7 Configure /home

Please note that home directories could be mounted anywhere and is not necessarily restricted to `/home` nor restricted to a single location nor is the name restricted in any way.

Checks can be made by looking in `/etc/passwd`, looking over the mounted file systems with `mount` or queering the relevant database with `getent`.

DRAFT

1.1.7.1 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:

The reasoning for mounting `/home` on a separate partition is as follow.

Protection from resource exhaustion

The default installation only creates a single `/` partition. Since the `/home` directory contains user generated data, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/home` and impact all local users.

Fine grained control over the mount

Configuring `/home` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limits an attackers ability to create exploits on the system. In the case of `/home` options such as `usrquota/grpquota` may be considered to limit the impact that users can have on each other with regards to disk resource exhaustion. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

Protection of user data

As `/home` contains user data, care should be taken to ensure the security and integrity of the data and mount point.

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 --kernel /home  
  
TARGET SOURCE FSTYPE OPTIONS  
/home /dev/sdb ext4 rw,relatime,seclabel
```

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/>

Additional Information:

When modifying `/home` 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 multi-user mode.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1038

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

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Verify that the `nodev` option is set for the `/home` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /home | grep nodev  
/home  /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/home` partition.

Example:

```
<device> /home      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/home` with the configured options:

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

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1022

1.1.7.3 Ensure nosuid option set on /home 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 `/home` filesystem is only intended for user file storage, set this option to ensure that users cannot create `setuid` files in `/home`.

Audit:

Verify that the `nosuid` option is set for the `/home` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /home | grep nosuid
/home  /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/home` partition.

Example:

```
<device> /home  <fstype>    defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/home` with the configured options:

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

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1022

1.1.7.4 Ensure usrquota option set on /home partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `usrquota` mount option allows for the filesystem to have disk quotas configured.

Rationale:

To ensure the availability of disk space on `/home`, it is important to limit the impact a single user or group can cause for other users (or the wider system) by accidentally filling up the partition. Quotas can also be applied to inodes for filesystems where inode exhaustion is a concern.

Audit:

Verify that the `usrquota` option is set for the `/home` mount, that quotas is enabled and configured.

Run the following command to verify that the `usrquota` mount option is set.

Example:

```
# findmnt --kernel /home | grep usrquota
/home    /dev/sdb ext4  rw,quota,usrquota,grpquota,nodev,relatime,seclabel
```

Run the following command to verify that the user quotas are enabled.

```
# quotaon -p /home | grep user
user quota on /home (/dev/sdb) is on
```

Remediation:

Edit the `/etc/fstab` file and add `usrquota` to the fourth field (mounting options) for the `/home` partition.

Example:

```
<device> /home      <fstype>      defaults,rw,usrquota,grpquota,nodev,relatime  
0 0
```

Run the following command to remount `/home` with the configured options:

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

Create the quota database. This example will ignore any existing quota files.

```
# quotacheck -cugv /home  
  
quotacheck: Your kernel probably supports journaled quota but you are not  
using it. Consider switching to journaled quota to avoid running quotacheck  
after an unclean shutdown.  
quotacheck: Scanning /dev/sdb [/home] done  
quotacheck: Cannot stat old user quota file /home/aquota.user: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Cannot stat old group quota file /home/aquota.group: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Cannot stat old user quota file /home/aquota.user: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Cannot stat old group quota file /home/aquota.group: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Checked 8 directories and 0 files  
quotacheck: Old file not found.  
quotacheck: Old file not found.
```

Restore SELinux context on the quota database files. Order of operations is important
as `quotaon` will set the immutable attribute on the files and thus `restorecon` will fail.

```
# restorecon /home/aquota.user
```

Enable quotas on the partition:

```
# quotaon -vug /home  
  
/dev/sdb [/home]: group quotas turned on  
/dev/sdb [/home]: user quotas turned on
```

References:

1. See the `fstab(5)` and `edquota(8)` manual pages for more information.

Additional Information:

Journal filesystems

If the destination filesystem is journaled, it is recommended to investigate the relevant documentation for the filesystem and use journaled quotas instead of the above example.

Setting quotas

Set the relevant quotas with `edquota`. See `man edquota` for more information.

Reporting

To see the current usage use `repquota -a`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.7.5 Ensure grpquota option set on /home partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `grpquota` mount option allows for the filesystem to have disk quotas configured.

Rationale:

To ensure the availability of disk space on `/home`, it is important to limit the impact a single user or group can cause for other users (or the wider system) by accidentally filling up the partition. Quotas can also be applied to inodes for filesystems where inode exhaustion is a concern.

Audit:

Verify that the `grpquota` option is set for the `/home` mount, that quotas is enabled and configured.

Run the following command to verify that the `grpquota` mount option is set.

Example:

```
# findmnt --kernel /home | grep grpquota
/home    /dev/sdb ext4  rw,quota,usrquota,grpquota,nodev,relatime,seclabel
```

Run the following command to verify that the user quotas are enabled.

```
# quotaon -p /home | grep group
user quota on /home (/dev/sdb) is on
```

Remediation:

Edit the `/etc/fstab` file and add `grpquota` to the fourth field (mounting options) for the `/home` partition.

Example:

```
<device> /home      <fstype>      defaults,rw,usrquota,grpquota,nodev,relatime  
0 0
```

Run the following command to remount `/home` with the configured options:

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

Create the quota database. This example will ignore any existing quota files.

```
# quotacheck -cugv /home  
  
quotacheck: Your kernel probably supports journaled quota but you are not  
using it. Consider switching to journaled quota to avoid running quotacheck  
after an unclean shutdown.  
quotacheck: Scanning /dev/sdb [/home] done  
quotacheck: Cannot stat old user quota file /home/aquota.user: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Cannot stat old group quota file /home/aquota.group: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Cannot stat old user quota file /home/aquota.user: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Cannot stat old group quota file /home/aquota.group: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Checked 8 directories and 0 files  
quotacheck: Old file not found.  
quotacheck: Old file not found.
```

Restore SELinux context on the quota database files. Order of operations is important
as `quotaon` will set the immutable attribute on the files and thus `restorecon` will fail.

```
# restorecon /home/aquota.group
```

Enable quotas on the partition:

```
# quotaon -vug /home  
  
/dev/sdb [/home]: group quotas turned on  
/dev/sdb [/home]: user quotas turned on
```

References:

1. See the `fstab(5)` and `edquota(8)` manual pages for more information.

Additional Information:

Journal filesystems

If the destination filesystem is journaled, it is recommended to investigate the relevant documentation for the filesystem and use journaled quotas instead of the above example.

Setting quotas

Set the relevant quotas with `edquota`. See `man edquota` for more information.

Reporting

To see the current usage use `repquota -a`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.8 Configure /dev/shm

DRAFT

1.1.8.1 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:

Verify that the `nodev` option is set for the `/dev/shm` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /dev/shm | grep noexec
```

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` using the updated options from `/etc/fstab`:

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

Additional Information:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1038

1.1.8.2 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:

Verify that the `noexec` option is set for the `/dev/shm` mount.

Run the following command to verify that the `noexec` mount option is set.

Example:

```
# findmnt --kernel /dev/shm | grep noexec
/dev/shm    tmpfs    tmpfs    rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/dev/shm` partition.

Example:

```
<device> /dev/shm      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
```

Run the following command to remount `/dev/shm` with the configured options:

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

NOTE It is recommended to use `tmpfs` as the device/filesystem type as `/dev/shm` is used as shared memory space by applications.

References:

1. See the `fstab(5)` manual page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0005	M1022

1.1.8.3 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:

Verify that the `nosuid` option is set for the `/dev/shm` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /dev/shm | grep 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` using the updated options from `/etc/fstab`:

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

Additional Information:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1038

1.1.9 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:

As a preference `autofs` should not be installed unless other packages depend on it. Run the following command to verify `autofs` is not installed:

```
# systemctl is-enabled autofs  
Failed to get unit file state for autofs.service: No such file or directory
```

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

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

Verify result is not "enabled".

Remediation:

If there are no other packages that depends on `autofs`, remove the package with:

```
# dnf remove autofs
```

Run the following command to disable `autofs` if it is required:

```
# systemctl --now disable 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
v7	<u>8.4 Configure Anti-Malware Scanning of Removable Devices</u> Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	●	●	●
v7	<u>8.5 Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1203, T1203.000, T1211, T1211.000, T1212, T1212.000		

1.1.10 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.

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/false  
# lsmod | grep usb-storage  
  
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf` with a line that reads `install usb-storage /bin/false` and a line that reads `blacklist usb-storage`.
Example:

```
# printf "install usb-storage /bin/false  
blacklist usb-storage  
" >> /etc/modprobe.d/usb-storage.conf
```

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

```
# modprobe -r usb-storage
```

Additional Information:

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

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>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.</p>	●	●	●
v7	<p>8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1052, T1052.001, T1091, T1091.000, T1200, T1200.000	TA0001, TA0010	M1034

1.2 Configure Software Updates

Ubuntu Linux uses 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.

DRAFT

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
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>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1195, T1195.001, T1195.002, T1203, T1203.000, T1210, T1210.000, T1211, T1211.000, T1212, T1212.000	TA0001	M1051

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
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>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1195, T1195.001, T1195.002	TA0001	M1051

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.

DRAFT

1.3.1 Ensure AIDE is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</p> <p>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>			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1036, T1036.002, T1036.003, T1036.004, T1036.005, T1565, T1565.001		

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
v7	<p>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</p> <p>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>			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1036, T1036.002, T1036.003, T1036.004, T1036.005, T1565, T1565.001	TA0040	M1022

1.4 Secure Boot Settings

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

DRAFT

1.4.1 Ensure bootloader password is set (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off 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 "^set superusers" /boot/grub/grub.cfg  
  
set superusers=<username>  
# grep "^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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1542, T1542.000	TA0003	M1046

1.4.2 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
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1542, T1542.000	TA0005, TA0007	M1022

1.4.3 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
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.000	TA0005	M1022

1.5 Additional Process Hardening

DRAFT

1.5.1 Ensure XD/NX support is enabled (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u></p> <p>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.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000	TA0002	M1050

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

Profile Applicability:

- Level 1 - Server
- Level 1 - 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u></p> <p>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.</p>	●		●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000	TA0002	M1050

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
v7	<p>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</p> <p>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>			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1055, T1055.009, T1065, T1065.001	TA0002	M1050

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
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0007	

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 Ubuntu L 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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1565, T1565.001, T1565.003	TA0003	M1026

1.6.1.2 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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1565, T1565.001, T1565.003	TA0003	M1026

1.6.1.3 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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
	TA0005	

1.6.1.4 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
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>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1565, T1565.001, T1565.003	TA0005	

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
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1082, T1082.000, T1592, T1592.004	TA0007	

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
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1082, T1082.000, T1592, T1592.004	TA0007	

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
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1018, T1018.000, T1082, T1082.000, T1592, T1592.004	TA0007	

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
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

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
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

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
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

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

DRAFT

1.8.1 Ensure GNOME Display Manager is removed (Automated)

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-query -W gdm3  
dpkg-query: no packages found matching gdm3
```

Remediation:

Run the following command to uninstall `gdm3`:

```
# apt purge gdm3
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1543, T1543.002	TA0002	

1.8.2 Ensure GDM login banner is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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:

Run the following script to verify that the text banner on the login screen is enabled and set:

```

#!/usr/bin/env bash

{
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package:
\"$l_pn\" exists on the system\n - checking configuration"
    done
    if [ -n "$l_pkgoutput" ]; then
        output="" output2=""
        # Look for existing settings and set variables if they exist
        l_gdmfile=$(grep -Prl '^h*banner-message-enable\b' /etc/dconf/db/*.d)
        if [ -n "$l_gdmfile" ]; then
            # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
            l_gdmprofile=$(awk -F'/' '{split($NF-1,a,".");print a[1]}' <<<
"$l_gdmfile")
            # Check if banner message is enabled
            if grep -Piq '^h*banner-message-enable=true\b' "$l_gdmfile"; then
                output="$output\n - The \"banner-message-enable\" option is enabled in
\"$l_gdmfile\""
            else
                output2="$output2\n - The \"banner-message-enable\" option is not enabled"
            fi
            l_lsbt=$(grep -Pios '^h*banner-message-text=.*$' "$l_gdmfile")
            if [ -n "$l_lsbt" ]; then
                output="$output\n - The \"banner-message-text\" option is set in
\"$l_gdmfile\"\n - banner-message-text is set to:\n - \"$l_lsbt\""
            else
                output2="$output2\n - The \"banner-message-text\" option is not set"
            fi
            if grep -Pq "h*system-db:$l_gdmprofile" /etc/dconf/profile/"$l_gdmprofile";
        then
            output="$output\n - The \"$l_gdmprofile\" profile exists"
        else
            output2="$output2\n - The \"$l_gdmprofile\" profile doesn't exist"
        fi
        if [ -f "/etc/dconf/db/$l_gdmprofile" ]; then
            output="$output\n - The \"$l_gdmprofile\" profile exists in the dconf
database"
        else
            output2="$output2\n - The \"$l_gdmprofile\" profile doesn't exist in the
dconf database"
        fi
    else
        output2="$output2\n - The \"banner-message-enable\" option isn't configured"
    fi
    if [ -z "$output2" ]; then
        echo -e "$l_pkgoutput\n- Audit result:\n    *** PASS: ***\n$output\n"
    else
        echo -e "$l_pkgoutput\n- Audit Result:\n    *** FAIL: ***\n$output2\n"
    fi
    else
        echo -e "\n\n - GNOME Desktop Manager isn't installed\n - Recommendation is Not
Applicable\n- Audit result:\n    *** PASS ***\n"
    fi
}

```

Remediation:

Run the following script to verify that the banner message is enabled and set:

DRAFT

```

#!/usr/bin/env bash

{
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pk in $l_pcl; do
        $l_pq "$l_pk" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package:
\"$l_pk\" exists on the system\n - checking configuration"
    done
    if [ -n "$l_pkgoutput" ]; then

        l_gdmprofile="gdm" # Set this to desired profile name IaW Local site policy
        l_bmessage="'Authorized uses only. All activity may be monitored and reported'"
        # Set to desired banner message
        if [ ! -f "/etc/dconf/profile/$l_gdmprofile" ]; then
            echo "Creating profile \"$l_gdmprofile\""
            echo -e "user-db:user\nsystem-db:$l_gdmprofile\nfile-
db:/usr/share/$l_gdmprofile/greeter-dconf-defaults" > /etc/dconf/profile/$l_gdmprofile
        fi
        if [ ! -d "/etc/dconf/db/$l_gdmprofile.d/" ]; then
            echo "Creating dconf database directory \"/etc/dconf/db/$l_gdmprofile.d/\""
            mkdir /etc/dconf/db/$l_gdmprofile.d/
        fi
        if ! grep -Piq '^h*banner-message-enable|h*=h*true\b'
        /etc/dconf/db/$l_gdmprofile.d/*; then
            echo "creating gdm keyfile for machine-wide settings"
            if ! grep -Piq -- '^h*banner-message-enable|h*' \
        /etc/dconf/db/$l_gdmprofile.d/*; then
                l_kfile="/etc/dconf/db/$l_gdmprofile.d/01-banner-message"
                echo -e "\n[org/gnome/login-screen]\nbanner-message-enable=true" >>
"$l_kfile"
            else
                l_kfile=$(grep -Pil -- '^h*banner-message-enable|h*' \
        /etc/dconf/db/$l_gdmprofile.d/*"
                    ! grep -Pq '^h*[org/gnome]/login-screen]' "$l_kfile" && sed -ri
                    '/^s*banner-message-enable/ i\[org/gnome/login-screen]' "$l_kfile"
                    ! grep -Pq '^h*banner-message-enable|h*=h*true\b' "$l_kfile" && sed -ri
                    's/^s*(banner-message-enable\s*=\s*)(\S+)(\s*.*)/\1true \3//' "$l_kfile"
                    #           sed -ri '/^s*[org/gnome]/login-screen]/ a\bnbanner-message-
                    enable=true' "$l_kfile"
                fi
            fi
            if ! grep -Piq "^h*banner-message-text=[\'\"]+\S+" "$l_kfile"; then
                sed -ri "/^s*banner-message-enable/ a\banner-message-text=$l_bmessage"
            fi
        dconf update
    else
        echo -e "\n\n - GNOME Desktop Manager isn't installed\n - Recommendation is Not
Applicable\n - No remediation required\n"
    fi
}

```

Note:

- There is no character limit for the banner message. gnome-shell autodetects longer stretches of text and enters two column mode.
- The banner message cannot be read from an external file.
OR

Run the following command to remove the gdm3 package:

```
# apt purge gdm3
```

Default Value:

disabled

References:

1. <https://help.gnome.org/admin/system-admin-guide/stable/login-banner.html.en>

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
	TA0007	

1.8.3 Ensure disable-user-list option 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 script and to verify that the `disable-user-list` option is enabled or GNOME isn't installed:

```

#!/usr/bin/env bash

{
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pk in $l_pcl; do
        $l_pq "$l_pk" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pk\" exists on the system\n - checking configuration"
    done
    if [ -n "$l_pkgoutput" ]; then
        output="" output2=""
        l_gdmfile=$(grep -Prl '^h*disable-user-list\h*\=\h*true\b' /etc/dconf/db)
        if [ -n "$l_gdmfile" ]; then
            output="$output\n - The \"disable-user-list\" option is enabled in \"$l_gdmfile\""
            l_gdmprofile=$(awk -F/ '{split($NF-1),a,".");print a[1]}' <<< "$l_gdmfile")
            if grep -Pq "^\h*system-db:$l_gdmprofile" /etc/dconf/profile/"$l_gdmprofile"; then
                output="$output\n - The \"$l_gdmprofile\" exists"
            else
                output2="$output2\n - The \"$l_gdmprofile\" doesn't exist"
            fi
            if [ -f "/etc/dconf/db/$l_gdmprofile" ]; then
                output="$output\n - The \"$l_gdmprofile\" profile exists in the dconf database"
            else
                output2="$output2\n - The \"$l_gdmprofile\" profile doesn't exist in the dconf database"
            fi
        else
            output2="$output2\n - The \"disable-user-list\" option is not enabled"
        fi
        if [ -z "$output2" ]; then
            echo -e "$l_pkgoutput\n- Audit result:\n      *** PASS: ***\n$output"
        else
            echo -e "$l_pkgoutput\n- Audit Result:\n      *** FAIL:\n***\n$output2\n"
        [ -n "$output" ] && echo -e "$output\n"
        fi
    else
        echo -e "\n\n - GNOME Desktop Manager isn't installed\n - Recommendation is Not Applicable\n- Audit result:\n      *** PASS ***\n"
    fi
}

```

Remediation:

Run the following script to enable the `disable-user-list` option:

Note: the `l_gdm_profile` variable in the script can be changed if a different profile name is desired in accordance with local site policy.

```
#!/usr/bin/env bash

{
    l_gdmprofile="gdm"
    if [ ! -f "/etc/dconf/profile/$l_gdmprofile" ]; then
        echo "Creating profile \"$l_gdmprofile\""
        echo -e "user-db:user\nsystem-db:$l_gdmprofile\nfile-
db:/usr/share/$l_gdmprofile/greeter-dconf-defaults" >
/etc/dconf/profile/$l_gdmprofile
    fi
    if [ ! -d "/etc/dconf/db/$l_gdmprofile.d/" ]; then
        echo "Creating dconf database directory
\"/etc/dconf/db/$l_gdmprofile.d/\""
        mkdir /etc/dconf/db/$l_gdmprofile.d/
    fi
    if ! grep -Piq '^h*disable-user-list\h*=\\h*true\\b'
/etc/dconf/db/$l_gdmprofile.d/*; then
        echo "creating gdm keyfile for machine-wide settings"
        if ! grep -Piq -- '^h*[org\\gnome\\login-screen\\]'
/etc/dconf/db/$l_gdmprofile.d/*; then
            echo -e "\n[org/gnome/login-screen]\n# Do not show the user
list\\ndisable-user-list=true" >> /etc/dconf/db/$l_gdmprofile.d/00-login-
screen
        else
            sed -ri '/^s*[org\\gnome\\login-screen\\]/ a\\# Do not show the user
list\\ndisable-user-list=true' $(grep -Pil -- '^h*[org\\gnome\\login-
screen\\]' /etc/dconf/db/$l_gdmprofile.d/*)
        fi
    fi
    dconf update
}
```

Note: When the user profile is created or changed, the user will need to log out and log in again before the changes will be applied.

OR

Run the following command to remove the GNOME package:

```
# apt purge gdm3
```

Default Value:

false

References:

1. <https://help.gnome.org/admin/system-admin-guide/stable/login-userlist-disable.html.en>

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1087, T1087.001, T1087.002	TA0007	M1028

1.8.4 Ensure GDM screen locks when the user is idle (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.

- `idle-delay=uint32 {n}` - Number of seconds of inactivity before the screen goes blank
- `lock-delay=uint32 {n}` - Number of seconds after the screen is blank before locking the screen

Example key file:

```
# Specify the dconf path
[org/gnome/desktop/session]

# Number of seconds of inactivity before the screen goes blank
# Set to 0 seconds if you want to deactivate the screensaver.
idle-delay=uint32 900

# Specify the dconf path
[org/gnome/desktop/screensaver]

# Number of seconds after the screen is blank before locking the screen
lock-delay=uint32 5
```

Rationale:

Setting a lock-out value reduces the window of opportunity for unauthorized user access to another user's session that has been left unattended.

Audit:

Run the following script to verify that the screen locks when the user is idle:

```

#!/usr/bin/env bash

{
    # Check if GNMOE Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -\nPackage: \"$l_pn\" exists on the system\n - checking configuration"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        l_idmv="900" # Set for max value for idle-delay in seconds
        l_ldmv="5" # Set for max value for lock-delay in seconds
        # Look for idle-delay to determine profile in use, needed for remaining
        tests
        l_kfile=$(grep -Psril '^h*idle-delay|h*=h*uint32|h+d+b' /etc/dconf/db/*) # Determine file containing idle-delay key
        if [ -n "$l_kfile" ]; then
            # set profile name (This is the name of a dconf database)
            l_profile=$(awk -F '/' '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile") #Set the key profile name
            l_pdbdir="/etc/dconf/db/$l_profile.d" # Set the key file dconf db
            directory
            # Confirm that idle-delay exists, includes unit32, and value is
            between 1 and max value for idle-delay
            l_idv=$(awk -F 'uint32' '/idle-delay/{print $2}' "$l_kfile" | xargs)"
            if [ -n "$l_idv" ]; then
                [ "$l_idv" -gt "0" -a "$l_idv" -le "$l_idmv" ] &&
                l_output="$l_output\n - The \"idle-delay\" option is set to \"$l_idv\" seconds in \"$l_kfile\""
                [ "$l_idv" = "0" ] && l_output2="$l_output2\n - The \"idle-
                delay\" option is set to \"$l_idv\" (disabled) in \"$l_kfile\""
                [ "$l_idv" -gt "$l_idmv" ] && l_output2="$l_output2\n - The
                \"idle-delay\" option is set to \"$l_idv\" seconds (greater than $l_idmv) in
                \"$l_kfile\""
            else
                l_output2="$l_output2\n - The \"idle-delay\" option is not set in
                \"$l_kfile\""
            fi
            # Confirm that lock-delay exists, includes unit32, and value is
            between 0 and max value for lock-delay
            l_ldv=$(awk -F 'uint32' '/lock-delay/{print $2}' "$l_kfile" | xargs)"
            if [ -n "$l_ldv" ]; then
                [ "$l_ldv" -ge "0" -a "$l_ldv" -le "$l_ldmv" ] &&
                l_output="$l_output\n - The \"lock-delay\" option is set to \"$l_ldv\""
            fi
        fi
    done
}

```

```

seconds in \"$l_kfile\""
      [ \"$l_ldv\" -gt \"$l_ldmv\" ] && l_output2=\"$l_output2\n - The
\"lock-delay\" option is set to \"$l_ldv\" seconds (greater than $l_ldmv) in
\"$l_kfile\""
    else
      l_output2=\"$l_output2\n - The \"lock-delay\" option is not set in
\"$l_kfile\""
    fi
  # Confirm that dconf profile exists
  if grep -Psq "^\h*system-db:$l_profile" /etc/dconf/profile/*; then
    l_output=\"$l_output\n - The \"$l_profile\" profile exists"
  else
    l_output2=\"$l_output2\n - The \"$l_profile\" doesn't exist"
  fi
  # Confirm that dconf profile database file exists
  if [ -f "/etc/dconf/db/$l_profile" ]; then
    l_output=\"$l_output\n - The \"$l_profile\" profile exists in the
dconf database"
  else
    l_output2=\"$l_output2\n - The \"$l_profile\" profile doesn't
exist in the dconf database"
  fi
  else
    l_output2=\"$l_output2\n - The \"idle-delay\" option doesn't exist,
remaining tests skipped"
  fi
else
  l_output=\"$l_output\n - GNOME Desktop Manager package is not installed
on the system\n - Recommendation is not applicable"
fi
# Report results. If no failures output in l_output2, we pass
[ -n "$l_pkgoutput" ] && echo -e "\n$l_pkgoutput"
if [ -z "$l_output2" ]; then
  echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
else
  echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
  [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
fi
}

```

Note:

- **idle-delay=uint32** Should be 900 seconds (15 minutes) or less, not 0 (disabled) and follow local site policy
- **lock-delay=uint32** should be 5 seconds or less and follow local site policy

Remediation:

Create or edit a file in the `/etc/dconf/profile/` and verify it includes the following:

```
user-db:user
system-db:{NAME_OF_DCONF_DATABASE}
```

Note: `local` is the name of a dconf database used in the examples.

Example:

```
# echo -e '\nuser-db:user\nsystem-db:local' >> /etc/dconf/profile/user
```

Create the directory `/etc/dconf/db/{NAME_OF_DCONF_DATABASE}.d/` if it doesn't already exist:

Example:

```
# mkdir /etc/dconf/db/local.d
```

Create the key file ``/etc/dconf/db/{NAME_OF_DCONF_DATABASE}.d/{FILE_NAME}`` to provide information for the `{NAME_OF_DCONF_DATABASE}` database:

Example script:

```
#!/usr/bin/env bash

l_key_file="/etc/dconf/db/local.d/00-screensaver"
l_idmv="900" # Set max value for idle-delay in seconds (between 1 and 900)
l_ldmv="5" # Set max value for lock-delay in seconds (between 0 and 5)
{
    echo '# Specify the dconf path'
    echo '[org/gnome/desktop/session]'
    echo ''
    echo '# Number of seconds of inactivity before the screen goes blank'
    echo '# Set to 0 seconds if you want to deactivate the screensaver.'
    echo "idle-delay=uint32 $l_idmv"
    echo ''
    echo '# Specify the dconf path'
    echo '[org/gnome/desktop/screensaver]'
    echo ''
    echo '# Number of seconds after the screen is blank before locking the
screen'
    echo "lock-delay=uint32 $l_ldmv"
} > "l_key_file"
```

Note: You must include the `uint32` along with the integer key values as shown.

Run the following command to update the system databases:

```
# dconf update
```

Note: Users must log out and back in again before the system-wide settings take effect.

References:

1. <https://help.gnome.org/admin/system-admin-guide/stable/desktop-lockscreens.html.en>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>4.3 Configure Automatic Session Locking on Enterprise Assets</u></p> <p>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.</p>	●	●	●
v7	<p><u>16.11 Lock Workstation Sessions After Inactivity</u></p> <p>Automatically lock workstation sessions after a standard period of inactivity.</p>	●	●	●

1.8.5 Ensure GDM screen locks cannot be overridden (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.

By using the lockdown mode in dconf, you can prevent users from changing specific settings.

To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.

Example Lock File:

```
# Lock desktop screensaver settings
/org/gnome/desktop/session/idle-delay
/org/gnome/desktop/screensaver/lock-delay
```

Rationale:

Setting a lock-out value reduces the window of opportunity for unauthorized user access to another user's session that has been left unattended.

Without locking down the system settings, user settings take precedence over the system settings.

Audit:

Run the following script to verify that the screen lock can not be overridden:

```

#!/usr/bin/env bash

{
    # Check if GNMOE Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - "
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        # Look for idle-delay to determine profile in use, needed for remaining
        tests
        l_kfd="/etc/dconf/db/${(grep -Psrl '^h*idle-'
        delay|h*uint32|h+d+b' /etc/dconf/db/*) | awk -F'/' '{split(${NF-}
        1,a,".");print a[1]}').d" #set directory of key file to be locked
        l_kfd2="/etc/dconf/db/${(grep -Psrl '^h*lock-'
        delay|h*uint32|h+d+b' /etc/dconf/db/*) | awk -F'/' '{split(${NF-}
        1,a,".");print a[1]}').d" #set directory of key file to be locked
        if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options
        can't be locked
            if grep -Prilq '/org/gnome/desktop/session/idle-delay\b' \
            "$l_kfd"; then
                l_output="$l_output\n - \"idle-delay\" is locked in \"$(grep -
                Pril '/org/gnome/desktop/session/idle-delay\b' \"$l_kfd\")\""
            else
                l_output2="$l_output2\n - \"idle-delay\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"idle-delay\" is not set so it can not be
            locked"
        fi
        if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist,
        options can't be locked
            if grep -Prilq '/org/gnome/desktop/screensaver/lock-delay\b' \
            "$l_kfd2"; then
                l_output="$l_output\n - \"lock-delay\" is locked in \"$(grep -
                Pril '/org/gnome/desktop/screensaver/lock-delay\b' \"$l_kfd2\")\""
            else
                l_output2="$l_output2\n - \"lock-delay\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"lock-delay\" is not set so it can not be
            locked"
        fi
    else
        l_output="$l_output\n - GNOME Desktop Manager package is not installed"
    fi
}

```

```
on the system\n  - Recommendation is not applicable"
fi
# Report results. If no failures output in l_output2, we pass
# [ -n "$l_pkgoutput" ] && echo -e "\n$l_pkgoutput"
if [ -z "$l_output2" ]; then
  echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
else
  echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
  [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
fi
}
```

Remediation:

Run the following script to ensure screen locks can not be overridden:

```

#!/usr/bin/env bash

{
    # Check if GNMOE Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable
    # determine system's package manager
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_dn in $l_pcl; do
        $l_pq "$l_dn" > /dev/null 2>&1 && l_pkgoutput="y" && echo -e "\n -
    Package: \"$l_dn\" exists on the system\n - remediating configuration if
    needed"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        # Look for idle-delay to determine profile in use, needed for remaining
        tests
        l_kfd="/etc/dconf/db/${(grep -Psril '^h*idle-
        delay|h*=h*uint32|h+d+b' /etc/dconf/db/*) | awk -F'/' '{split(${NF-
        1},a,".");print a[1]}').d" #set directory of key file to be locked
        # Look for lock-delay to determine profile in use, needed for remaining
        tests
        l_kfd2="/etc/dconf/db/${(grep -Psril '^h*lock-
        delay|h*=h*uint32|h+d+b' /etc/dconf/db/*) | awk -F'/' '{split(${NF-
        1},a,".");print a[1]}').d" #set directory of key file to be locked
        if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options
        can't be locked
            if grep -Prilq '^h*/org/gnome/desktop/session/idle-delay\b' "$l_kfd"; then
                echo " - \"idle-delay\" is locked in \"$(grep -Pril
                '^h*/org/gnome/desktop/session/idle-delay\b' "$l_kfd")\""
            else
                echo "creating entry to lock \"idle-delay\""
                [ ! -d "$l_kfd"/locks ] && echo "creating directory $l_kfd/locks"
                && mkdir "$l_kfd"/locks
                {
                    echo '# Lock desktop screensaver idle-delay setting'
                    echo '/org/gnome/desktop/session/idle-delay'
                } >> "$l_kfd"/locks/00-screensaver
            fi
        else
            echo -e " - \"idle-delay\" is not set so it can not be locked\n -
        Please follow Recommendation \"Ensure GDM screen locks when the user is
        idle\" and follow this Recommendation again"
        fi
        if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist,
        options can't be locked
            if grep -Prilq '^h*/org/gnome/desktop/screensaver/lock-
            delay\b' "$l_kfd2"; then
                echo " - \"lock-delay\" is locked in \"$(grep -Pril
                '^h*/org/gnome/desktop/screensaver/lock-delay\b' "$l_kfd2")\""
            fi
        fi
    fi
}

```

```

        else
            echo "creating entry to lock \"lock-delay\""
            [ ! -d "$l_kfd2"/locks ] && echo "creating directory
$l_kfd2/locks" && mkdir "$l_kfd2"/locks
        {
            echo '# Lock desktop screensaver lock-delay setting'
            echo '/org/gnome/desktop/session/idle-delay'
        } >> "$l_kfd2"/locks/00-screensaver
    fi
else
    echo -e " - \"lock-delay\" is not set so it can not be locked\n -
Please follow Recommendation \"Ensure GDM screen locks when the user is
idle\" and follow this Recommendation again"
    fi
else
    echo -e " - GNOME Desktop Manager package is not installed on the
system\n - Recommendation is not applicable"
    fi
}

```

Run the following command to update the system databases:

```
# dconf update
```

Note: Users must log out and back in again before the system-wide settings take effect.

References:

1. <https://help.gnome.org/admin/system-admin-guide/stable/desktop-lockscreens.html.en>
2. <https://help.gnome.org/admin/system-admin-guide/stable/dconf-lockdown.html.en>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	<u>16.11 Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

1.8.6 Ensure automatic mounting of removable media is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

By default GNOME automatically mounts removable media when inserted as a convenience to the user.

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:

IF GNOME Desktop Manager is installed, run the following command to verify automatic mounting is disabled:

```
# gsettings get org.gnome.desktop.media-handling automount  
false
```

Verify result is "false".

Remediation:

Ensure that automatic mounting of media is disabled for all GNOME users:

```
# cat << EOF >> /etc/dconf/db/local.d/00-media-automount  
[org/gnome/desktop/media-handling]  
automount=false  
automount-open=false  
EOF
```

Apply the changes with:

```
# dconf update
```

OR

Run the following command to uninstall the GNOME desktop Manager package:

```
# dnf uninstall gdm
```

References:

1. <https://access.redhat.com/solutions/20107>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>10.3 Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	<u>8.5 Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.	●	●	●

1.8.7 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	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</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 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1056, T1056.001, T1557, T1557.000	TA0002	M1050

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
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.

DRAFT

2.1 Configure 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`.

Note:

- 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
 - `chrony` should be removed from the system
 - `ntp` should be removed from the system

2.1.1 Ensure time synchronization is in use

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`.

Note:

- 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
 - `chrony` should be removed from the system
 - `ntp` should be removed from the system

2.1.1.1 Ensure a single time synchronization daemon 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.

Note:

- **On virtual systems where host based time synchronization is available consult your virtualization software documentation and verify that host based synchronization is in use and follows local site policy. In this scenario, this section should be skipped**
- Only **one** time synchronization method should be in use on the system. Configuring multiple time synchronization methods could lead to unexpected or unreliable results

Rationale:

Time synchronization is important to support time sensitive security mechanisms and ensures log files have consistent time records across the enterprise, which aids in forensic investigations.

Audit:

On physical systems, and virtual systems where host based time synchronization is not available.

One of the three time synchronization daemons should be available; **chrony**, **systemd-timesyncd**, or **ntp**

Run the following script to verify that a single time synchronization daemon is available on the system:

```
#!/usr/bin/env bash

{
    output="" l_tsdt="" l_sdtd="" chrony="" l_ntp=""
    dpkg-query -W chrony > /dev/null 2>&1 && l_chrony="y"
    dpkg-query -W ntp > /dev/null 2>&1 && l_ntp="y" || l_ntp=""
    systemctl list-units --all --type=service | grep -q 'systemd-timesyncd.service' && systemctl is-enabled systemd-timesyncd.service | grep -q 'enabled' && l_sdtd="y"
    # ! systemctl is-enabled systemd-timesyncd.service | grep -q 'enabled' &&
    l_nsdt="y" || l_nsdt=""
    if [[ "$l_chrony" = "y" && "$l_ntp" != "y" && "$l_sdtd" != "y" ]]; then
        l_tsdt="chrony"
        output="$output\n- chrony is in use on the system"
    elif [[ "$l_chrony" != "y" && "$l_ntp" = "y" && "$l_sdtd" != "y" ]]; then
        l_tsdt="ntp"
        output="$output\n- ntp is in use on the system"
    elif [[ "$l_chrony" != "y" && "$l_ntp" != "y" ]]; then
        if systemctl list-units --all --type=service | grep -q 'systemd-timesyncd.service' && systemctl is-enabled systemd-timesyncd.service | grep -Eq '(enabled|disabled|masked)'; then
            l_tsdt="sdtd"
            output="$output\n- systemd-timesyncd is in use on the system"
        fi
    else
        [[ "$l_chrony" = "y" && "$l_ntp" = "y" ]] && output="$output\n- both chrony and ntp are in use on the system"
        [[ "$l_chrony" = "y" && "$l_sdtd" = "y" ]] && output="$output\n- both chrony and systemd-timesyncd are in use on the system"
        [[ "$l_ntp" = "y" && "$l_sdtd" = "y" ]] && output="$output\n- both ntp and systemd-timesyncd are in use on the system"
    fi
    if [ -n "$l_tsdt" ]; then
        echo -e "\n- PASS:\n$output\n"
    else
        echo -e "\n- FAIL:\n$output\n"
    fi
}
```

NOTE: Follow the guidance in the subsection for the time synchronization daemon available on the system and skip the other two time synchronization daemon subsections.

Remediation:

On physical systems, and virtual systems where host based time synchronization is not available.

Select **one** of the three time synchronization daemons; `chrony` (1), `systemd-timesyncd` (2), or `ntp` (3), and following the remediation procedure for the selected daemon.

Note: enabling more than one synchronization daemon could lead to unexpected or unreliable results:

1. chrony

Run the following command to install `chrony`:

```
# apt install chrony
```

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

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

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

Run the following command to remove the `ntp` package:

```
# apt purge ntp
```

NOTE:

- Subsection: **Configure chrony** should be followed
- Subsections: **Configure systemd-timesyncd** and **Configure ntp** should be skipped

2. systemd-timesyncd

Run the following command to remove the `chrony` package:

```
# apt purge chrony
```

Run the following command to remove the `ntp` package:

```
# apt purge ntp
```

NOTE:

- Subsection: **Configure systemd-timesyncd** should be followed
- Subsections: **Configure chrony** and **Configure ntp** should be skipped

3. ntp

Run the following command to install `ntp`:

```
# apt install ntp
```

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

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

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

Run the following command to remove the `chrony` package:

```
# apt purge chrony
```

NOTE:

- Subsection: **Configure ntp** should be followed
- Subsections: **Configure chrony** and **Configure systemd-timesyncd** should be skipped

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.001	TA0005	

2.1.2 Configure chrony

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.

chrony can be configured to be a client and/or a server.

More information on chrony can be found at: <http://chrony.tuxfamily.org/>.

Note:

- If ntp or systemd-timesyncd are used, chrony should be removed and this section skipped
- Only one time synchronization method should be in use on the system

2.1.2.1 Ensure chrony is configured with authorized timeserver (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

- server
 - The server directive specifies an NTP server which can be used as a time source. The client-server relationship is strictly hierarchical: a client might synchronize its system time to that of the server, but the server's system time will never be influenced by that of a client.
 - This directive can be used multiple times to specify multiple servers.
 - The directive is immediately followed by either the name of the server, or its IP address.
- pool
 - The syntax of this directive is similar to that for the server directive, except that it is used to specify a pool of NTP servers rather than a single NTP server. The pool name is expected to resolve to multiple addresses which might change over time.
 - This directive can be used multiple times to specify multiple pools.
 - All options valid in the server directive can be used in this directive too.

Rationale:

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Audit:

IF chrony is in use on the system, run the following command to display the server and/or pool directive:

```
# grep -Pr --include=*.{sources,conf} '^h*(server|pool)\h+\H+' /etc/chrony/
```

Verify that at least one pool line and/or at least three server lines are returned, and the timeserver on the returned lines follows local site policy

Output examples:

pool directive:

```
pool time.nist.gov iburst maxsources 4 #The maxsources option is unique to  
the pool directive
```

server directive:

```
server time-a-g.nist.gov iburst  
server 132.163.97.3 iburst  
server time-d-b.nist.gov iburst
```

Remediation:

Edit `/etc/chrony/chrony.conf` or a file ending in `.sources` in `/etc/chrony/sources.d/` and add or edit server or pool lines as appropriate according to local site policy:

```
<[server|pool]> <[remote-server|remote-pool]>
```

Examples:

pool directive:

```
pool time.nist.gov iburst maxsources 4 #The maxsources option is unique to  
the pool directive
```

server directive:

```
server time-a-g.nist.gov iburst  
server 132.163.97.3 iburst  
server time-d-b.nist.gov iburst
```

Run one of the following commands to load the updated time sources into `chrony` running config:

```
# systemctl restart chrony  
- OR if sources are in a .sources file -  
# chronyc reload sources
```

OR

If another time synchronization service is in use on the system, run the following command to remove `chrony` from the system:

```
# apt purge chrony
```

References:

1. `chrony.conf(5)` Manual Page
2. <https://tf.nist.gov/tf-cgi/servers.cgi>

Additional Information:

If pool and/or server directive(s) are set in a sources file in `/etc/chrony/sources.d`, the line:

```
sourcedir /etc/chrony/sources.d
```

must be present in `/etc/chrony/chrony.conf`

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.001	TA0002	M1022

2.1.2.2 Ensure chrony is running as user _chrony (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `chrony` package is installed with a dedicated user account `_chrony`. This account is granted the access required by the `chronyd` service

Rationale:

The `chronyd` service should run with only the required priviliges

Audit:

IF `chrony` is in use on the system, run the following command to verify the `chronyd` service is being run as the `_chrony` user:

```
# ps -ef | awk '/([c]hronyd)/ && $1!="_chrony") { print $1 }'
```

Nothing should be returned

Remediation:

Add or edit the `user` line to `/etc/chrony/chrony.conf` or a file ending in `.conf` in `/etc/chrony/conf.d/`:

```
user _chrony
```

OR

If another time synchronization service is in use on the system, run the following command to remove `chrony` from the system:

```
# apt purge chrony
```

Default Value:

`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.		●	●

2.1.2.3 Ensure chrony is enabled and running (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

chrony is a daemon for synchronizing the system clock across the network

Rationale:

chrony needs to be enabled and running in order to synchronize the system to a timeserver.

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Audit:

IF chrony is in use on the system, run the following commands:

Run the following command to verify that the `chrony` service is enabled:

```
# systemctl is-enabled chrony.service  
enabled
```

Run the following command to verify that the `chrony` service is active:

```
# systemctl is-active chrony.service  
active
```

Remediation:

IF chrony is in use on the system, run the following commands:

Run the following command to unmask chrony.service:

```
# systemctl unmask chrony.service
```

Run the following command to enable and start chrony.service:

```
# systemctl --now enable chrony.service
```

OR

If another time synchronization service is in use on the system, run the following command to remove chrony:

```
# apt purge 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.		●	●

2.1.3 Configure systemd-timesyncd

`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`.

The default configuration is set during compilation, so configuration is only needed when it is necessary to deviate from those defaults. Initially, the main configuration file in `/etc/systemd/` contains commented out entries showing the defaults as a guide to the administrator. Local overrides can be created by editing this file or by creating drop-ins, as described below. Using drop-ins for local configuration is recommended over modifications to the main configuration file.

In addition to the "main" configuration file, drop-in configuration snippets are read from `/usr/lib/systemd/.conf.d/`, `/usr/local/lib/systemd/.conf.d/`, and `/etc/systemd/*.conf.d/`. Those drop-ins have higher precedence and override the main configuration file. Files in the `*.conf.d/` configuration subdirectories are sorted by their filename in lexicographic order, regardless of in which of the subdirectories they reside. When multiple files specify the same option, for options which accept just a single value, the entry in the file sorted last takes precedence, and for options which accept a list of values, entries are collected as they occur in the sorted files.

When packages need to customize the configuration, they can install drop-ins under `/usr/`. Files in `/etc/` are reserved for the local administrator, who may use this logic to override the configuration files installed by vendor packages. Drop-ins have to be used to override package drop-ins, since the main configuration file has lower precedence. It is recommended to prefix all filenames in those subdirectories with a two-digit number and a dash, to simplify the ordering of the files.

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.

Note:

- The recommendations in this section only apply if timesyncd is in use on the system
- 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
- **If chrony or ntp are used, systemd-timesyncd should be stopped and masked, and this section skipped**
- **One, and only one, time synchronization method should be in use on the system**

DRAFT

2.1.3.1 Ensure systemd-timesyncd configured with authorized timeserver (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

NTP=

- A space-separated list of NTP server host names or IP addresses. During runtime this list is combined with any per-interface NTP servers acquired from `systemd-networkd.service(8)`. `systemd-timesyncd` will contact all configured system or per-interface servers in turn, until one responds. When the empty string is assigned, the list of NTP servers is reset, and all prior assignments will have no effect. This setting defaults to an empty list.

FallbackNTP=

- A space-separated list of NTP server host names or IP addresses to be used as the fallback NTP servers. Any per-interface NTP servers obtained from `systemd-networkd.service(8)` take precedence over this setting, as do any servers set via `NTP=` above. This setting is hence only relevant if no other NTP server information is known. When the empty string is assigned, the list of NTP servers is reset, and all prior assignments will have no effect. If this option is not given, a compiled-in list of NTP servers is used.

Rationale:

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Audit:

IF `systemd-timesyncd` is in use on the system, run the following command:

```
# find /etc/systemd -type f -name '*.conf' -exec grep -Ph  
'^h*(NTP|FallbackNTP)=\H+' {} +
```

Verify that `NPT=<space_separated_list_of_servers>` and/or
`FallbackNTP=<space_separated_list_of_servers>` is returned and that the time
server(s) shown follows local site policy

Example Output:

```
/etc/systemd/timesyncd.conf.d/50-timesyncd.conf:NTP=time.nist.gov  
/etc/systemd/timesyncd.conf.d/50-timesyncd.conf:FallbackNTP=time-a-g.nist.gov  
time-b-g.nist.gov time-c-g.nist.gov
```

Remediation:

Edit or create a file in /etc/systemd/timesyncd.conf.d ending in .conf and add the NTP= and/or FallbackNTP= lines to the [Time] section:

Example:

```
[Time]
NTP=time.nist.gov # Uses the generic name for NIST's time servers
-AND/OR-
FallbackNTP=time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov # Space
separated list of NIST time servers
```

Note: Servers added to these line(s) should follow local site policy. NIST servers are for example. The timesyncd.conf.d directory may need to be created

Example script: The following example script will create the systemd-timesyncd drop-in configuration snippet:

```
#!/usr/bin/env bash

ntp_ts="time.nist.gov"
ntp_fb="time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov"
disfile="/etc/systemd/timesyncd.conf.d/50-timesyncd.conf"
if ! find /etc/systemd -type f -name '*.conf' -exec grep -Ph '^h*NTP=\H+' {} +
; then
    [ ! -d /etc/systemd/timesyncd.conf.d ] && mkdir
/etc/systemd/timesyncd.conf.d
    ! grep -Pqs '^h*\[Time\]' "$disfile" && echo "[Time]" >> "$disfile"
    echo "NTP=$ntp_ts" >> "$disfile"
fi
if ! find /etc/systemd -type f -name '*.conf' -exec grep -Ph
'^h*FallbackNTP=\H+' {} +; then
    [ ! -d /etc/systemd/timesyncd.conf.d ] && mkdir
/etc/systemd/timesyncd.conf.d
    ! grep -Pqs '^h*\[Time\]' "$disfile" && echo "[Time]" >> "$disfile"
    echo "FallbackNTP=$ntp_fb" >> "$disfile"
fi
```

Run the following command to reload the systemd-timesyncd configuration:

```
# systemctl try-reload-or-restart systemd-timesyncd
```

OR

If another time synchronization service is in use on the system, run the following command to stop and mask systemd-timesyncd:

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

Default Value:

#NTP=

#FallbackNPT=

References:

1. <https://www.freedesktop.org/software/systemd/man/timesyncd.conf.html>
2. <https://tf.nist.gov/tf-cgi/servers.cgi>

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.001	TA0002	M1022

2.1.3.2 Ensure systemd-timesyncd is enabled and running (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

Rationale:

systemd-timesyncd needs to be enabled and running in order to synchronize the system to a timeserver.

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Audit:

IF systemd-timesyncd is in use on the system, run the following commands:

Run the following command to verify that the `systemd-timesyncd` service is enabled:

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

Run the following command to verify that the `systemd-timesyncd` service is active:

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

Remediation:

IF `systemd-timesyncd` is in use on the system, run the following commands:
Run the following command to unmask `systemd-timesyncd.service`:

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

Run the following command to enable and start `systemd-timesyncd.service`:

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

OR

If another time synchronization service is in use on the system, run the following command to stop and mask `systemd-timesyncd`:

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

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.		●	●

2.1.4 Configure ntp

`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.

Note:

- 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**

2.1.4.1 Ensure ntp access control is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

ntp Access Control Commands:

```
restrict address [mask mask] [ippeerlimit int] [flag ...]
```

The `address` argument expressed in dotted-quad form is the address of a host or network. Alternatively, the `address` argument can be a valid host DNS name.

The `mask` argument expressed in dotted-quad form defaults to 255.255.255.255, meaning that the address is treated as the address of an individual host. A default entry (address 0.0.0.0, mask 0.0.0.0) is always included and is always the first entry in the list. **Note:** the text string `default`, with no mask option, may be used to indicate the default entry.

The `ippeerlimit` directive limits the number of peer requests for each IP to `int`, where a value of -1 means "unlimited", the current default. A value of 0 means "none". There would usually be at most 1 peering request per IP, but if the remote peering requests are behind a proxy there could well be more than 1 per IP. In the current implementation, flag always restricts access, i.e., an entry with no flags indicates that free access to the server is to be given.

The flags are not orthogonal, in that more restrictive flags will often make less restrictive ones redundant. The flags can generally be classed into two categories, those which restrict time service and those which restrict informational queries and attempts to do run-time reconfiguration of the server.

One or more of the following flags may be specified:

- `kod` - If this flag is set when an access violation occurs, a kiss-o'-death (KoD) packet is sent. KoD packets are rate limited to no more than one per second. If another KoD packet occurs within one second after the last one, the packet is dropped.
- `limited` - Deny service if the packet spacing violates the lower limits specified in the `discard` command. A history of clients is kept using the monitoring capability of `ntpd`. Thus, monitoring is always active as long as there is a restriction entry with the `limited` flag.
- `lowpriotrap` - Declare traps set by matching hosts to be low priority. The number of traps a server can maintain is limited (the current limit is 3). Traps are usually assigned on a first come, first served basis, with later trap requestors being denied service. This flag modifies the assignment algorithm by allowing low priority traps to be overridden by later requests for normal priority traps.
- `noepeer` - Deny ephemeral peer requests, even if they come from an authenticated source. Note that the ability to use a symmetric key for authentication may be restricted to one or more IPs or subnets via the third field of the `ntp.keys` file. This restriction is not enabled by default, to maintain backward compatibility. Expect `noepeer` to become the default in `ntp-4.4`.
- `nomodify` - Deny `ntpq` and `ntpdc` queries which attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.
- `noquery` - Deny `ntpq` and `ntpdc` queries. Time service is not affected.
- `nopeer` - Deny unauthenticated packets which would result in mobilizing a new association. This includes broadcast and symmetric active packets when a configured association does not exist. It also includes pool associations, so if you want to use servers from a pool directive and also want to use `nopeer` by default, you'll want a `restrict source ...` line as well that does not include the `nopeer` directive.
- `noserve` - Deny all packets except `ntpq` and `ntpdc` queries.
- `notrap` - Decline to provide mode 6 control message trap service to matching hosts. The trap service is a subsystem of the `ntpq` control message protocol which is intended for use by remote event logging programs.
- `notrust` - Deny service unless the packet is cryptographically authenticated.
- `ntpport` - This is actually a match algorithm modifier, rather than a restriction flag. Its presence causes the restriction entry to be matched only if the source port in the packet is the standard NTP UDP port (123). Both `ntpport` and `non-ntpport` may be specified. The `ntpport` is considered more specific and is sorted later in the list.

Rationale:

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

Audit:

If ntp is in use on the system, run the following command to verify the restrict lines:

```
# grep -P -- '^h*restrict\h+((-4\h+)?|-6\h+)default\h+(:[^#\n\r]+\h+)*(!(:\2|\3|\4|\5))(\h*\bkod\b\h*|\h*\bnomodify\b\h*|\h*\bnotrap\b\h*|\h*\bnopeer\b\h*|\h*\bnoquery\b\h*)\h+(:[^#\n\r]+\h+)*(!(:\1|\3|\4|\5))(\h*\bkod\b\h*|\h*\bnomodify\b\h*|\h*\bnotrap\b\h*|\h*\bnopeer\b\h*|\h*\bnoquery\b\h*)\h+(:[^#\n\r]+\h+)*(!(:\1|\2|\4|\5))(\h*\bkod\b\h*|\h*\bnomodify\b\h*|\h*\bnotrap\b\h*|\h*\bnopeer\b\h*|\h*\bnoquery\b\h*)\h+(:[^#\n\r]+\h+)*(!(:\1|\2|\3|\5))(\h*\bkod\b\h*|\h*\bnomodify\b\h*|\h*\bnotrap\b\h*|\h*\bnopeer\b\h*|\h*\bnoquery\b\h*)\h+(:[^#\n\r]+\h+)*(!(:\1|\2|\3|\4))(\h*\bkod\b\h*|\h*\bnomodify\b\h*|\h*\bnotrap\b\h*|\h*\bnopeer\b\h*|\h*\bnoquery\b\h*)\h*(?:\h+\H+\h*)*(?:\h+\#.*?)$' /etc/ntp.conf
```

Output should be similar to:

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

Verify that the output includes two lines, and both lines include: default, kod, nomodify, notrap, nopeer and noquery.

Note: The -4 in the first line is optional, options after default may appear in any order, and additional options may exist.

Remediation:

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
```

OR

If another time synchronization service is in use on the system, run the following command to remove ntp from the system:

```
# apt purge ntp
```

Default Value:

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

References:

1. <http://www.ntp.org/>
2. ntp.conf(5)
3. ntpd(8)

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.		●	●

2.1.4.2 Ensure ntp is configured with authorized timeserver (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The various modes are determined by the command keyword and the type of the required IP address. Addresses are classed by type as (s) a remote server or peer (IPv4 class A, B and C), (b) the broadcast address of a local interface, (m) a multicast address (IPv4 class D), or (r) a reference clock address (127.127.x.x).

Note: That only those options applicable to each command are listed below. Use of options not listed may not be caught as an error, but may result in some weird and even destructive behavior.

If the Basic Socket Interface Extensions for IPv6 (RFC-2553) is detected, support for the IPv6 address family is generated in addition to the default support of the IPv4 address family. In a few cases, including the reslist billboard generated by `ntpq` or `ntpdc`, IPv6 addresses are automatically generated. IPv6 addresses can be identified by the presence of colons ":" in the address field. IPv6 addresses can be used almost everywhere where IPv4 addresses can be used, with the exception of reference clock addresses, which are always IPv4.

Note: In contexts where a host name is expected, a -4 qualifier preceding the host name forces DNS resolution to the IPv4 namespace, while a -6 qualifier forces DNS resolution to the IPv6 namespace. See IPv6 references for the equivalent classes for that address family.

- pool - For type s addresses, this command mobilizes a persistent client mode association with a number of remote servers. In this mode the local clock can synchronize to the remote server, but the remote server can never be synchronized to the local clock.
- server - For type s and r addresses, this command mobilizes a persistent client mode association with the specified remote server or local radio clock. In this mode the local clock can synchronize to the remote server, but the remote server can never be synchronized to the local clock. This command should not be used for type b or m addresses.

Rationale:

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Audit:

If ntp is in use on the system, run the following command to display the server and/or pool mode:

```
# grep -P -- '^h*(server|pool)\h+H+' /etc/ntp.conf
```

Verify that at least one pool line and/or at least three server lines are returned, and the timeserver on the returned lines follows local site policy

Output examples:

pool mode:

```
pool time.nist.gov iburst maxsources 4 #The maxsources option is unique to  
the pool directive
```

server mode:

```
server time-a-g.nist.gov iburst  
server 132.163.97.3 iburst  
server time-d-b.nist.gov iburst
```

Remediation:

Edit /etc/ntp.conf and add or edit server or pool lines as appropriate according to local site policy:

```
<[server|pool]> <[remote-server|remote-pool]>
```

Examples:

pool mode:

```
pool time.nist.gov iburst
```

server mode:

```
server time-a-g.nist.gov iburst  
server 132.163.97.3 iburst  
server time-d-b.nist.gov iburst
```

Run the following command to load the updated time sources into ntp running config:

```
# systemctl restart ntp
```

OR

If another time synchronization service is in use on the system, run the following command to remove ntp from the system:

```
# apt purge ntp
```

References:

1. <http://www.ntp.org/>
2. <https://tf.nist.gov/tf-cgi/servers.cgi>
3. ntp.conf(5)
4. ntpd(8)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.</p>		●	●
v7	<p>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.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1498, T1498.002, T1562, T1562.001	TA0002	M1022

2.1.4.3 Ensure ntp is running as user ntp (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `ntp` package is installed with a dedicated user account `ntp`. This account is granted the access required by the `ntpd` daemon

Note:

- 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:

The `ntpd` daemon should run with only the required privilege

Audit:

IF `ntp` is in use on the system run the following command to verify the `ntpd` daemon is being run as the user `ntp`:

```
# ps -ef | awk '/([n]tpd)/ && $1!="ntp") { print $1 }'
```

Nothing should be returned

Run the following command to verify the `RUNASUSER=` is set to `ntp` in `/etc/init.d/ntp`:

```
# grep -P -- '^h*RUNASUSER=' /etc/init.d/ntp
RUNASUSER=ntp
```

Remediation:

Add or edit the following line in `/etc/init.d/ntp`:

```
RUNASUSER=ntp
```

Run the following command to restart `ntp.service`:

```
# systemctl restart ntp.service
```

OR

If another time synchronization service is in use on the system, run the following command to remove `ntp` from the system:

```
# apt purge ntp
```

Default Value:

user ntp

References:

1. <http://www.ntp.org/>

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.		●	●

2.1.4.4 Ensure ntp is enabled and running (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

ntp is a daemon for synchronizing the system clock across the network

Rationale:

ntp needs to be enabled and running in order to synchronize the system to a timeserver.

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Audit:

IF ntp is in use on the system, run the following commands:

Run the following command to verify that the ntp service is enabled:

```
# systemctl is-enabled ntp.service  
enabled
```

Run the following command to verify that the ntp service is active:

```
# systemctl is-active ntp.service  
active
```

Remediation:

IF ntp is in use on the system, run the following commands:

Run the following command to unmask `ntp.service`:

```
# systemctl unmask ntp.service
```

Run the following command to enable and start `ntp.service`:

```
# systemctl --now enable ntp.service
```

OR

If another time synchronization service is in use on the system, run the following command to remove `ntp`:

```
# apt purge 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.		●	●

2.2 Special Purpose Services

This section describes services that are installed on systems that specifically need to run these services. If any of these services are not required, it is recommended that they be 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>
```

DRAFT

2.2.1 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
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.3 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
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.4 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
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.5 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.6 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
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.7 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.8 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.9 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.10 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.11 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
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000, T1039, T1039.000, T1083, T1083.000, T1135, T1135.000, T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	

2.2.12 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.13 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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.14 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.15 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` 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1018, T1018.000, T1210, T1210.000	TA0008	M1042

2.2.16 Ensure rsync service is either not installed or masked (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
```

OR

Run the following commands to verify that `rsync` is inactive and masked:

```
# systemctl is-active rsync  
inactive  
  
# systemctl is-enabled rsync  
masked
```

Remediation:

Run the following command to remove `rsync`:

```
# apt purge rsync
```

OR

Run the following commands to stop and mask `rsync`:

```
# systemctl stop rsync
```

```
# systemctl mask rsync
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1105, T1105.000, T1203, T1203.000, T1210, T1210.000, T1543, T1543.002, T1570, T1570.000	TA0008	M1042

2.3 Service Clients

A number of insecure services exist. While disabling the servers prevents a local attack against these services, it is advised to remove their clients unless they are required.

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

DRAFT

2.3.1 Ensure NIS Client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client 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
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1543, T1543.002	TA0008	M1042

2.3.2 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
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1203, T1203.000, T1543, T1543.002	TA0008	M1041, M1042

2.3.3 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
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1543, T1543.002	TA0006, TA0008	M1041, M1042

2.3.4 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
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1203, T1203.000, T1543, T1543.002	TA0006, TA0008	M1041, M1042

2.3.5 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
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1543, T1543.002	TA0008	M1042

2.3.6 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1543, T1543.002	TA0008	M1042

2.4 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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

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.

Note:

- sysctl settings are defined through files in `/usr/lib/sysctl.d/`, `/run/sysctl.d/`, and `/etc/sysctl.d/`.
- Files must have the ".conf" extension.
- Vendors settings live in `/usr/lib/sysctl.d/`
- To override a whole file, create a new file with the same name in `/etc/sysctl.d/` and put new settings there.
- To override only specific settings, add a file with a lexically later name in `/etc/sysctl.d/` and put new settings there.
- The paths where sysctl preload files usually exist
 - `/run/sysctl.d/*.conf`
 - `/etc/sysctl.d/*.conf`
 - `/usr/local/lib/sysctl.d/*.conf`
 - `/usr/lib/sysctl.d/*.conf`
 - `/lib/sysctl.d/*.conf`
 - `/etc/sysctl.conf`

3.1 Disable unused network protocols and devices

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

DRAFT

3.1.1 Ensure system is checked to determine if IPv6 is enabled (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Internet Protocol Version 6 (IPv6) is the most recent version of Internet Protocol (IP). It's designed to supply IP addressing and additional security to support the predicted growth of connected devices. IPv6 is based on 128-bit addressing and can support 340 undecillion, which is 340 trillion³ addresses.

Features of IPv6

- Hierarchical addressing and routing infrastructure
- Stateful and Stateless configuration
- Support for quality of service (QoS)
- An ideal protocol for neighboring node interaction

Rationale:

IETF RFC 4038 recommends that applications are built with an assumption of dual stack. It is recommended that IPv6 be enabled and configured in accordance with Benchmark recommendations.

If dual stack and IPv6 are not used in your environment, IPv6 may be disabled to reduce the attack surface of the system, and recommendations pertaining to IPv6 can be skipped.

Impact:

ETF RFC 4038 recommends that applications are built with an assumption of dual stack. Disabling IPv6 on the system may cause some applications to fail or have unexpected behavior.

Audit:

Run the following script to verify IPv6 status on the system:

```
#!/usr/bin/env bash

{
    output=""
    grubfile=$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg' \) -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"

    if [ -s "$grubfile" ]; then
        ! grep -P -- "^\h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
ipv6.disable=1 && output="IPv6 Disabled in \"$grubfile\""
        fi

    if grep -Pqs -- "^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)? $" $searchloc && \
grep -Pqs --
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)? $" $searchloc &&
\
        sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)? $" && \
        sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)? $"; then
            [ -n "$output" ] && output="$output, and in sysctl config" ||
output="ipv6 disabled in sysctl config"
        fi

    [ -n "$output" ] && echo -e "\n$output\n" || echo -e "\nIPv6 is enabled on
the system\n"
}
```



Remediation:

It is recommended that IPv6 be enabled and configured in accordance with Benchmark recommendations. If IPv6 is to be disabled, use **one** of the two following methods to disable IPv6 on the system:

To disable IPv6 through the GRUB2 config, run the following command to add `ipv6.disable=1` to the `GRUB_CMDLINE_LINUX` parameters:

Edit `/etc/default/grub` and add `ipv6.disable=1` to the `GRUB_CMDLINE_LINUX` parameters:

Example:

```
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:

Example:

```
# printf "
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
" >> /etc/sysctl.d/60-disable_ipv6.conf
```

Run the following command 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
}
```

Default Value:

IPv6 is enabled

Additional Information:

Having more addresses has grown in importance with the expansion of smart devices and connectivity. IPv6 provides more than enough globally unique IP addresses for every networked device currently on the planet, helping ensure providers can keep pace with the expected proliferation of IP-based devices.

NIST SP 800-53 Rev. 5:

- CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</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 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000, T1595, T1595.001, T1595.002	TA0008	M1042

3.1.2 Ensure wireless interfaces are disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

Wireless networking is used when wired networks are unavailable. Ubuntu Linux contains a wireless tool kit to allow system administrators to configure and use wireless networks.

Rationale:

If wireless is not to be used, wireless devices can be disabled to reduce the potential attack surface.

Impact:

Many if not all laptop workstations and some desktop workstations will connect via wireless requiring these interfaces be enabled.

Audit:

Run the following 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
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1011, T1011.000, T1595, T1595.001, T1595.002	TA0010	M1028

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 script to verify packet redirect sending is disabled:

```
#!/usr/bin/env bash

{
    KPC()
    {
        kpname=$(awk -F= '{print $1}' <<< "$kpe")
        kpvalue=$(awk -F= '{print $2}' <<< "$kpe")
        krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
        pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?\$"
$searchloc)"
        fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'"
        if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ];
then
            echo -e "\nPASS:\n\"$kpname\" is set to \"$kpvalue\" in the
running configuration and in \"$pafile\""
        else
            echo -e "\nFAIL:"
            [ "$krp" != "$kpvalue" ] && echo -e "\"$kpname\" is set to
\"$krp\" in the running configuration"
            [ -n "$fafile" ] && echo -e "\"$kpname\" is set incorrectly in
\"$fafile\""
            [ -z "$pafile" ] && echo -e "\"$kpname = $kpvalue\" is not set in
a kernel parameter configuration file"
        fi
    }
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    for kpe in net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.default.send_redirects=0; do
        KPC
    done
}
```

Remediation:

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

Example:

```
# printf "  
net.ipv4.conf.all.send_redirects = 0  
net.ipv4.conf.default.send_redirects = 0  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command 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  
}
```

Default Value:

`net.ipv4.conf.all.send_redirects = 1`

`net.ipv4.conf.default.send_redirects = 1`

Additional Information:

NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</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 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0006, TA0009	M1030, M1042

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 script to verify IP forwarding is disabled:

```

#!/usr/bin/env bash

{
    KPC()
    {
        kpname=$(awk -F= '{print $1}' <<< "$kpe")
        kpvalue=$(awk -F= '{print $2}' <<< "$kpe")
        krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
        pafile=$(grep -Psl -- '^h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$' $searchloc)
        fofile=$(grep -s -- '^s*$kpname' $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F= '{print $1}')
        if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fofile" ]; then
            echo -e "\nPASS:\n\$kpname is set to \$kpvalue in the running
configuration and in \$pafile"
        else
            echo -e "\nFAIL:"
            [ "$krp" != "$kpvalue" ] && echo -e "\$kpname is set to \$krp in the
running configuration"
            [ -n "$fofile" ] && echo -e "\$kpname is set incorrectly in
\$fofile"
            [ -z "$pafile" ] && echo -e "\$kpname = \$kpvalue is not set in a kernel
parameter configuration file"
        fi
    }
    check_ipv6()
    {
        output=""
        grubfile=$(find /boot -type f \(-name 'grubenv' -o -name 'grub.conf' -o -name
'grub.cfg' \) -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)
        if [ -s "$grubfile" ]; then
            ! grep -P -- '^h*(kernelopts=|linux|kernel)' "$grubfile" | grep -vq --
ipv6.disable=1 && output="disabled"
        fi
        if grep -Pqs -- '^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$$'
$searchloc && \
            grep -Pqs -- '^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$$'
$searchloc && \
            sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- \
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$$" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- \
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$$"; then
            output="disabled"
        fi
        if [ -n "$output" ]; then
            echo -e "IPv6 disabled on the system, \$kpe is not applicable"
        else
            KPC
        fi
    }
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    for kpe in net.ipv4.ip_forward=0 net.ipv6.conf.all.forwarding=0; do
        if grep -q '^net.ipv6.' <<< "$kpe"; then
            check_ipv6
        else
            KPC
        fi
    done
}

```

Remediation:

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

Example:

```
# printf "  
net.ipv4.ip_forward = 0  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {  
    sysctl -w net.ipv4.ip_forward=0  
    sysctl -w net.ipv4.route.flush=1  
}
```

IF IPv6 is enabled on the system:

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

Example:

```
# printf "  
net.ipv6.conf.all.forwarding = 0  
" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {  
    sysctl -w net.ipv6.conf.all.forwarding=0  
    sysctl -w net.ipv6.route.flush=1  
}
```

Default Value:

`net.ipv4.ip_forward = 0`

`net.ipv6.conf.all.forwarding = 0`

Additional Information:

NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</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 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0006, TA0009	M1030, M1042

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 script to verify source routed packets are not accepted:

```

#!/usr/bin/env bash

{
    KPC()
    {
        kpname=$(awk -F= '{print $1}' <<< "$kpe")
        kpvalue=$(awk -F= '{print $2}' <<< "$kpe")
        krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
        pafile=$(grep -Psl -- '^h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$' $searchloc)
        fofile=$(grep -s -- '^s*$kpname' $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F= '{print $1}')
        if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fofile" ]; then
            echo -e "\nPASS:\n\$kpname is set to \$kpvalue in the running
configuration and in \$pafile"
        else
            echo -e "\nFAIL:"
            [ "$krp" != "$kpvalue" ] && echo -e "\$kpname is set to \$krp in the
running configuration"
            [ -n "$fofile" ] && echo -e "\$kpname is set incorrectly in
\$fofile"
            [ -z "$pafile" ] && echo -e "\$kpname = \$kpvalue is not set in a kernel
parameter configuration file"
        fi
    }
    check_ipv6()
    {
        output=""
        grubfile=$(find /boot -type f \(-name 'grubenv' -o -name 'grub.conf' -o -name
'grub.cfg' \) -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)
        if [ -s "$grubfile" ]; then
            ! grep -P -- '^h*(kernelopts=|linux|kernel)' "$grubfile" | grep -vq --
ipv6.disable=1 && output="disabled"
        fi
        if grep -Pqs -- '^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$$'
$searchloc && \
            grep -Pqs -- '^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$$'
$searchloc && \
            sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- \
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$$" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- \
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$$"; then
            output="disabled"
        fi
        if [ -n "$output" ]; then
            echo -e "IPv6 disabled on the system, \$kpe is not applicable"
        else
            KPC
        fi
    }
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    for kpe in net.ipv4.conf.all.accept_source_route=0
net.ipv4.conf.default.accept_source_route=0 net.ipv6.conf.all.accept_source_route=0
net.ipv6.conf.default.accept_source_route=0; do
        if grep -q '^net.ipv6.' <<< "$kpe"; then
            check_ipv6
        else
            KPC
        fi
    done
}

```

Remediation:

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

Example:

```
# printf "  
net.ipv4.conf.all.accept_source_route = 0  
net.ipv4.conf.default.accept_source_route = 0  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command 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 on the system:

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

Example:

```
# printf "  
net.ipv6.conf.all.accept_source_route = 0  
net.ipv6.conf.default.accept_source_route = 0  
" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command 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  
}
```

Default Value:

```
net.ipv4.conf.all.accept_source_route = 0  
net.ipv4.conf.default.accept_source_route = 0  
net.ipv6.conf.all.accept_source_route = 0  
net.ipv6.conf.default.accept_source_route = 0
```

Additional Information:

NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</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 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1590, T1590.005	TA0007	

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 script to verify ICMP redirects are not accepted:

```

#!/usr/bin/env bash

{
    KPC()
    {
        kpname=$(awk -F= '{print $1}' <<< "$kpe")
        kpvalue=$(awk -F= '{print $2}' <<< "$kpe")
        krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
        pafile=$(grep -Psl -- '^h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$' $searchloc)
        fofile=$(grep -s -- '^s*$kpname' $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F= '{print $1}')
        if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fofile" ]; then
            echo -e "\nPASS:\n\$kpname is set to \$kpvalue in the running
configuration and in \$pafile"
        else
            echo -e "\nFAIL:"
            [ "$krp" != "$kpvalue" ] && echo -e "\$kpname is set to \$krp in the
running configuration"
            [ -n "$fofile" ] && echo -e "\$kpname is set incorrectly in
\$fofile"
            [ -z "$pafile" ] && echo -e "\$kpname = \$kpvalue is not set in a kernel
parameter configuration file"
        fi
    }
    check_ipv6()
    {
        output=""
        grubfile=$(find /boot -type f \(-name 'grubenv' -o -name 'grub.conf' -o -name
'grub.cfg' \) -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)
        if [ -s "$grubfile" ]; then
            ! grep -P -- '^h*(kernelopts=|linux|kernel)' "$grubfile" | grep -vq --
ipv6.disable=1 && output="disabled"
        fi
        if grep -Pqs -- '^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$$'
$searchloc && \
            grep -Pqs -- '^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$$'
$searchloc && \
            sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs -- \
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$$" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs -- \
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$$"; then
            output="disabled"
        fi
        if [ -n "$output" ]; then
            echo -e "IPv6 disabled on the system, \$kpe is not applicable"
        else
            KPC
        fi
    }
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    for kpe in net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0 net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0; do
        if grep -q '^net.ipv6.' <<< "$kpe"; then
            check_ipv6
        else
            KPC
        fi
    done
}

```

Remediation:

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

Example:

```
# printf "  
net.ipv4.conf.all.accept_redirects = 0  
net.ipv4.conf.default.accept_redirects = 0  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command 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 on the system:

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

Example:

```
# printf "  
net.ipv6.conf.all.accept_redirects = 0  
net.ipv6.conf.default.accept_redirects = 0  
" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command 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  
}
```

Default Value:

```
net.ipv4.conf.all.accept_redirects = 1  
net.ipv4.conf.default.accept_redirects = 1  
net.ipv6.conf.all.accept_redirects = 1  
net.ipv6.conf.default.accept_redirects = 1
```

Additional Information:

NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</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 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0006, TA0009	M1030, M1042

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 script to verify secure ICMP redirects are not accepted:

```
#!/usr/bin/env bash

{
    KPC()
    {
        kpname=$(awk -F= '{print $1}' <<< "$kpe")
        kpvalue=$(awk -F= '{print $2}' <<< "$kpe")
        krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
        pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?\$"
$searchloc)"
        fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'"
        if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ];
then
            echo -e "\nPASS:\n\"$kpname\" is set to \"$kpvalue\" in the
running configuration and in \"$pafile\""
        else
            echo -e "\nFAIL:"
            [ "$krp" != "$kpvalue" ] && echo -e "\"$kpname\" is set to
\"$krp\" in the running configuration"
            [ -n "$fafile" ] && echo -e "\"$kpname\" is set incorrectly in
\"$fafile\""
            [ -z "$pafile" ] && echo -e "\"$kpname = $kpvalue\" is not set in
a kernel parameter configuration file"
        fi
    }
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    for kpe in net.ipv4.conf.all.secure_redirects=0
net.ipv4.conf.default.secure_redirects=0; do
        KPC
    done
}
```

Remediation:

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

Example:

```
# printf "  
net.ipv4.conf.all.secure_redirects = 0  
net.ipv4.conf.default.secure_redirects = 0  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

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  
}
```

Default Value:

`net.ipv4.conf.all.secure_redirects = 1`

`net.ipv4.conf.default.secure_redirects = 1`

Additional Information:

NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</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 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0006, TA0009	M1030, M1042

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 script to verify suspicious packets are logged:

```
#!/usr/bin/env bash

{
    KPC()
    {
        kpname=$(awk -F= '{print $1}' <<< "$kpe")
        kpvalue=$(awk -F= '{print $2}' <<< "$kpe")
        krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
        pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?\$"
$searchloc)"
        fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'"
        if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ];
then
            echo -e "\nPASS:\n\"$kpname\" is set to \"$kpvalue\" in the
running configuration and in \"$pafile\""
        else
            echo -e "\nFAIL:"
            [ "$krp" != "$kpvalue" ] && echo -e "\"$kpname\" is set to
\"$kpvalue\" in the running configuration"
            [ -n "$fafile" ] && echo -e "\"$kpname\" is set incorrectly in
\"$fafile\""
            [ -z "$pafile" ] && echo -e "\"$kpname = $kpvalue\" is not set in
a kernel parameter configuration file"
        fi
    }
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    for kpe in net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1; do
        KPC
    done
}
```

Remediation:

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

Example:

```
# printf "  
net.ipv4.conf.all.log_martians = 1  
net.ipv4.conf.default.log_martians = 1  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command 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  
}
```

Default Value:

`net.ipv4.conf.all.log_martians = 0`

`net.ipv4.conf.default.log_martians = 0`

Additional Information:

NIST SP 800-53 Rev. 5:

- AU-3
- AU-3(1)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.</p>		●	●
v7	<p>6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p>6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	

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 script to verify broadcast ICMP requests are ignored:

```
#!/usr/bin/env bash

{
    KPC()
    {
        kpname=$(awk -F= '{print $1}' <<< "$kpe")
        kpvalue=$(awk -F= '{print $2}' <<< "$kpe")
        krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
        pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)? $" $searchloc)
        fofile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv -- "\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}')
        if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fofile" ];
        then
            echo -e "\nPASS:\n\"$kpname\" is set to \"$kpvalue\" in the
running configuration and in \"$pafile\""
        else
            echo -e "\nFAIL:"
            [ "$krp" != "$kpvalue" ] && echo -e "\"$kpname\" is set to
\"$krp\" in the running configuration"
            [ -n "$fofile" ] && echo -e "\"$kpname\" is set incorrectly in
\"$fofile\""
            [ -z "$pafile" ] && echo -e "\"$kpname = $kpvalue\" is not set in
a kernel parameter configuration file"
        fi
    }
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    kpe="net.ipv4.icmp_echo_ignore_broadcasts=1"
    KPC
}
}
```

Remediation:

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

Example:

```
# printf "
net.ipv4.icmp_echo_ignore_broadcasts = 1
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
    sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
    sysctl -w net.ipv4.route.flush=1
}
```

Default Value:

`net.ipv4.conf.default.log_martians = 0`

Additional Information:

NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1498, T1498.001	TA0040	M1037

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:

```
#!/usr/bin/env bash

{
    KPC()
    {
        kpname=$(awk -F= '{print $1}' <<< "$kpe")
        kpvalue=$(awk -F= '{print $2}' <<< "$kpe")
        krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
        pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)? $" $searchloc)
        fofile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv -- "\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}')
        if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fofile" ];
        then
            echo -e "\nPASS:\n\"$kpname\" is set to \"$kpvalue\" in the
running configuration and in \"$pafile\""
        else
            echo -e "\nFAIL:"
            [ "$krp" != "$kpvalue" ] && echo -e "\"$kpname\" is set to
\"$krp\" in the running configuration"
            [ -n "$fofile" ] && echo -e "\"$kpname\" is set incorrectly in
\"$fofile\""
            [ -z "$pafile" ] && echo -e "\"$kpname = $kpvalue\" is not set in
a kernel parameter configuration file"
        fi
    }
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    kpe="net.ipv4.icmp_ignore_bogus_error_responses=1"
    KPC
}
}
```

Remediation:

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

Example:

```
# printf "
net.ipv4.icmp_ignore_bogus_error_responses = 1
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
    sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
    sysctl -w net.ipv4.route.flush=1
}
```

Default Value:

`net.ipv4.icmp_ignore_bogus_error_responses = 1`

Additional Information:

NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0040	M1053

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 script to verify Reverse Path Filtering is enabled:

```
#!/usr/bin/env bash

{
    KPC()
    {
        kpname=$(awk -F= '{print $1}' <<< "$kpe")
        kpvalue=$(awk -F= '{print $2}' <<< "$kpe")
        krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
        pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?\$"
$searchloc)"
        fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'"
        if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ];
then
            echo -e "\nPASS:\n\"$kpname\" is set to \"$kpvalue\" in the
running configuration and in \"$pafile\""
        else
            echo -e "\nFAIL:"
            [ "$krp" != "$kpvalue" ] && echo -e "\"$kpname\" is set to
\"$krp\" in the running configuration"
            [ -n "$fafile" ] && echo -e "\"$kpname\" is set incorrectly in
\"$fafile\""
            [ -z "$pafile" ] && echo -e "\"$kpname = $kpvalue\" is not set in
a kernel parameter configuration file"
        fi
    }
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    for kpe in net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1; do
        KPC
    done
}

```

Remediation:

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

Example:

```
# printf "  
net.ipv4.conf.all.rp_filter = 1  
net.ipv4.conf.default.rp_filter = 1  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

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  
}
```

Default Value:

`net.ipv4.conf.all.rp_filter = 2`

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

Additional Information:

NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</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 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1498, T1498.001	TA0006, TA0040	M1030, M1042

3.3.8 Ensure TCP SYN Cookies is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

When `tcp_syncookies` is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

Rationale:

Attackers use SYN flood attacks to perform a denial of service attack on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Audit:

Run the following script to verify TCP SYN Cookies is enabled:

```
#!/usr/bin/env bash

{
    KPC()
    {
        kpname=$(awk -F= '{print $1}' <<< "$kpe")
        kpvalue=$(awk -F= '{print $2}' <<< "$kpe")
        krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
        pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$" $searchloc)
        fofile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv -- "\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}')
        if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fofile" ];
        then
            echo -e "\nPASS:\n\"$kpname\" is set to \"$kpvalue\" in the
running configuration and in \"$pafile\""
        else
            echo -e "\nFAIL:"
            [ "$krp" != "$kpvalue" ] && echo -e "\"$kpname\" is set to
\"$krp\" in the running configuration"
            [ -n "$fofile" ] && echo -e "\"$kpname\" is set incorrectly in
\"$fofile\""
            [ -z "$pafile" ] && echo -e "\"$kpname = $kpvalue\" is not set in
a kernel parameter configuration file"
        fi
    }
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    kpe="net.ipv4.tcp_syncookies=1"
    KPC
}
}
```

Remediation:

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

Example:

```
# printf "
net.ipv4.tcp_syncookies = 1
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

Default Value:

`net.ipv4.tcp_syncookies = 1`

Additional Information:

NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0040	M1037

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:

Run the following script to verify IPv6 router advertisements are not accepted:

```

#!/usr/bin/env bash

{
    KPC()
    {
        kpname=$(awk -F= '{print $1}' <<< "$kpe")
        kpvalue=$(awk -F= '{print $2}' <<< "$kpe")
        krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
        pafile=$(grep -Psl -- '^h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$' $searchloc)
        fofile=$(grep -s -- '^s*$kpname' $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F= '{print $1}')
        if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fofile" ]; then
            echo -e "\nPASS:\n\$kpname is set to \$kpvalue in the running
configuration and in \$pafile"
        else
            echo -e "\nFAIL:"
            [ "$krp" != "$kpvalue" ] && echo -e "\$kpname is set to \$krp in the
running configuration"
            [ -n "$fofile" ] && echo -e "\$kpname is set incorrectly in
\$fofile"
            [ -z "$pafile" ] && echo -e "\$kpname = \$kpvalue is not set in a kernel
parameter configuration file"
        fi
    }
    check_ipv6()
    {
        output=""
        grubfile=$(find /boot -type f \(-name 'grubenv' -o -name 'grub.conf' -o -name
'grub.cfg' \) -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)
        if [ -s "$grubfile" ]; then
            ! grep -P -- '^h*(kernelopts=|linux|kernel)' "$grubfile" | grep -vq --
ipv6.disable=1 && output="disabled"
        fi
        if grep -Pqs -- '^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$$'
$searchloc && \
            grep -Pqs -- '^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$$'
$searchloc && \
            sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$$" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$$"; then
            output="disabled"
        fi
        if [ -n "$output" ]; then
            echo -e "IPv6 disabled on the system, \$kpe is not applicable"
        else
            KPC
        fi
    }
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    for kpe in net.ipv6.conf.all.accept_ra=0 net.ipv6.conf.default.accept_ra=0; do
        if grep -q '^net.ipv6.' <<< "$kpe"; then
            check_ipv6
        else
            KPC
        fi
    done
}

```

Remediation:

IF IPv6 is enabled on the system:

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

Example:

```
# printf "  
net.ipv6.conf.all.accept_ra = 0  
net.ipv6.conf.default.accept_ra = 0  
" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command 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  
}
```

Default Value:

`net.ipv6.conf.all.accept_ra = 1`

`"net.ipv6.conf.default.accept_ra = 1`

Additional Information:

NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</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 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0006, TA0040	M1030, M1042

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.

DRAFT

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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

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.

Note:

- *Only one method should be used to configure a firewall on the system. Use of more than one method could produce unexpected results*
- *This section is intended only to ensure the resulting firewall rules are in place, not how they are configured*

3.5.1 Configure UncomplicatedFirewall

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

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
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

3.5.1.3 Ensure ufw service is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - 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 the `ufw` daemon is enabled:

```
# systemctl is-enabled ufw.service  
enabled
```

Run the following command to verify that the `ufw` daemon is active:

```
# systemctl is-active ufw  
active
```

Run the following command to verify ufw is active

```
# ufw status  
Status: active
```

Remediation:

Run the following command to unmask the `ufw` daemon:

```
# systemctl unmask ufw.service
```

Run the following command to enable and start the `ufw` daemon:

```
# systemctl --now enable ufw.service  
active
```

Run the following command to enable ufw:

```
# ufw enable
```

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
	TA0011	M1031, M1037

3.5.1.6 Ensure ufw 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.

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 script to verify a firewall rule exists for all open ports:

```
#!/usr/bin/env bash

ufw_out=$(ufw status verbose)
ss -tuln | awk '($5!~/%lo:/ && $5!~/127.0.0.1:/ && $5!~/:1/) {split($5, a,
":"); print a[2]}' | sort | uniq | while read -r lpn; do
    ! grep -Pq "\h*$lpn\b" <<< "$ufw_out" && echo "- Port: \"$lpn\" is
missing a firewall rule"
done
```

Nothing should be returned

Remediation:

For each port identified in the audit which does not have a firewall rule, add rule for accepting or denying inbound connections:

Example:

```
# 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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

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 out http <- required for apt to connect to repository
ufw allow in https
ufw allow out 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** , **reject** , or **disabled**:

```
# ufw status verbose | grep Default:
```

Example output:

```
Default: deny (incoming), deny (outgoing), disabled (routed)
```

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
v7	<u>9.4 Apply Host-based Firewalls or Port Filtering</u> 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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

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.

Note:

- *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 below 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"
```

DRAFT

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.

Note:

- *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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562	TA0011	M1031, M1037

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031

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.

DRAFT

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

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
v7	<u>9.4 Apply Host-based Firewalls or Port Filtering</u> 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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	

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 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
v7	<u>9.4 Apply Host-based Firewalls or Port Filtering</u> 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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.5.3.2.2 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
v7	<u>9.4 Apply Host-based Firewalls or Port Filtering</u> 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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.5.3.2.3 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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
	TA0011	M1031, M1037

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 INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out      source
destination
  0     0 ACCEPT     all  --  lo      *      0.0.0.0/0      0.0.0.0/0
  0     0 DROP       all  --  *       *      127.0.0.0/8    0.0.0.0/0
  0     0 ACCEPT     tcp  --  *       *      0.0.0.0/0      0.0.0.0/0
tcp dpt:22 state NEW
```

Verify all open ports listening on non-localhost addresses have at least one firewall rule.
The last line identified by the "tcp dpt:22 state NEW" identifies it as a firewall rule for new connections on tcp port 22.

Remediation:

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j
ACCEPT
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><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.</p>		●	●
v7	<p><u>9.4 Apply Host-based Firewalls or Port Filtering</u> 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>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

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 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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.5.3.3.2 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" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eq "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eq
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

Remediation:

Run the following commands to implement 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
v7	<u>9.4 Apply Host-based Firewalls or Port Filtering</u> 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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.5.3.3.3 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
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.	●	●	●
v6	9.1 Limit Open Ports, Protocols, and Services Ensure that only ports, protocols, and services with validated business needs are running on each system.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
	TA0011	M1031, M1037

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
v7	<u>9.4 Apply Host-based Firewalls or Port Filtering</u> <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>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

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 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. A centralized log server provides a single point of entry for further analysis, monitoring and filtering.

Security principals for logging

- Ensure transport layer security is implemented between the client and the log server.
- Ensure that logs are rotated as per the environment requirements.
- Ensure all locally generated logs have the appropriate permissions.
- Ensure all security logs are sent to a remote log server.
- Ensure the required events are logged.

What is covered

This section will cover the minimum best practices for the usage of **either rsyslog or journald**. The recommendations are written such that each is wholly independent of each other and **only one is implemented**.

- If your organization makes use of an enterprise wide logging system completely outside of `rsyslog` or `journald`, then the following recommendations does not directly apply. However, the principals of the recommendations should be followed regardless of what solution is implemented. If the enterprise solution incorporates either of these tools, careful consideration should be given to the following recommendations to determine exactly what applies.
- Should your organization make use of both `rsyslog` and `journald`, take care how the recommendations may or may not apply to you.

What is not covered

- Enterprise logging systems not utilizing `rsyslog` or `journald`. As logging is very situational and dependent on the local environment, not everything can be covered here.
- Transport layer security should be applied to all remote logging functionality. Both `rsyslog` and `journald` supports secure transport and should be configured as such.
- The log server. There are a multitude of reasons for a centralized log server (and keeping a short period logging on the local system), but the log server is out of scope for these recommendations.

4.1.1 Configure journald

Included in the systemd suite is a journaling service called `systemd-journald.service` for the collection and storage of logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources such as:

- Classic RFC3164 BSD syslog via the `/dev/log` socket
- STDOUT/STDERR of programs via `StandardOutput=journal + StandardError=journal` in service files (both of which are default settings)
- Kernel log messages via the `/dev/kmsg` device node
- Audit records via the kernel's audit subsystem
- Structured log messages via journald's native protocol

Any changes made to the `systemd-journald` configuration will require a re-start of `systemd-journald`

4.1.1.1 Ensure journald is configured to send logs to a remote log host

DRAFT

4.1.1.1.1 Ensure systemd-journal-remote is installed (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

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:

Verify `systemd-journal-remote` is installed.

Run the following command:

```
# dpkg -s systemd-journal-remote
```

Verify the output matches:

```
# systemd-journal-remote-<version>
```

Remediation:

Run the following command to install `systemd-journal-remote`:

```
# apt install systemd-journal-remote
```

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

4.1.1.1.2 Ensure systemd-journal-remote is configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

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:

Verify `systemd-journal-remote` is configured.

Run the following command:

```
# grep -P "^(?:(?!\s*#).)*URL=|^(?:(?!\s*#).)*ServerKeyFile=|^(?:(?!\s*#).)*ServerCertificateFile=|^(?:(?!\s*#).)*TrustedCertificateFile=" /etc/systemd/journal-upload.conf
```

Verify the output matches per your environments certificate locations and the URL of the log server. Example:

```
URL=192.168.50.42
ServerKeyFile=/etc/ssl/private/journal-upload.pem
ServerCertificateFile=/etc/ssl/certs/journal-upload.pem
TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Remediation:

Edit the `/etc/systemd/journal-upload.conf` file and ensure the following lines are set per your environment:

```
URL=192.168.50.42  
ServerKeyFile=/etc/ssl/private/journal-upload.pem  
ServerCertificateFile=/etc/ssl/certs/journal-upload.pem  
TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Restart the service:

```
# systemctl restart systemd-journal-upload
```

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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

4.1.1.1.3 Ensure systemd-journal-remote is enabled (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

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:

Verify `systemd-journal-remote` is enabled.

Run the following command:

```
# systemctl is-enabled systemd-journal-upload.service
```

Verify the output matches:

```
enabled
```

Remediation:

Run the following command to enable `systemd-journal-remote`:

```
# systemctl --now enable systemd-journal-upload.service
```

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

4.1.1.1.4 Ensure journald is not configured to receive logs from a remote client (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Journald supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

NOTE:

- The same package, `systemd-journal-remote`, is used for both sending logs to remote hosts and receiving incoming logs.
- With regards to receiving logs, there are two services; `systemd-journal-remote.socket` and `systemd-journal-remote.service`.

Rationale:

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside its operational boundary.

Audit:

Run the following command to verify `systemd-journal-remote.socket` is not enabled:

```
# systemctl is-enabled systemd-journal-remote.socket
```

Verify the output matches:

```
disabled
```

Remediation:

Run the following command to disable `systemd-journal-remote.socket`:

```
# systemctl --now disable systemd-journal-remote.socket
```

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.		●	●
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.		●	●
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

4.1.1.2 Ensure journald service is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Ensure that the `systemd-journald` service is enabled to allow capturing of logging events.

Rationale:

If the `systemd-journald` service is not enabled to start on boot, the system will not capture logging events.

Audit:

Run the following command to verify `systemd-journald` is enabled:

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

Verify the output matches:

```
static
```

Remediation:

By default the `systemd-journald` service does not have an `[Install]` section and thus cannot be enabled / disabled. It is meant to be referenced as `Requires` or `Wants` by other unit files. As such, if the status of `systemd-journald` is not static, investigate why.

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.001	TA0005	

4.1.1.3 Ensure journald is configured to compress large log files (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The journald system includes the capability of compressing overly large files to avoid filling up the system with logs or making the logs unmanageably large.

Rationale:

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

Audit:

Review `/etc/systemd/journald.conf` and verify that large files will be compressed:

```
# grep ^\s*Compress /etc/systemd/journald.conf
```

Verify the output matches:

```
Compress=yes
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
Compress=yes
```

Restart the service:

```
# systemctl restart systemd-journald
```

Additional Information:

The main configuration file `/etc/systemd/journald.conf` is read before any of the custom `*.conf` files. If there are custom configs present, they override the main configuration parameters.

It is possible to change the default threshold of 512 bytes per object before compression is used.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
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.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.002	TA0040	M1053

4.1.1.4 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 due to a reboot.

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 ^\s*Storage /etc/systemd/journald.conf
```

Verify the output matches:

```
Storage=persistent
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
Storage=persistent
```

Restart the service:

```
# systemctl restart systemd-journald
```

Additional Information:

The main configuration file `/etc/systemd/journald.conf` is read before any of the custom `*.conf` files. If there are custom configs present, they override the main configuration parameters.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0005	M1022

4.1.1.5 Ensure journald is not configured to send logs to rsyslog (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Data from `journald` should be kept in the confines of the service and not forwarded on to other services.

Rationale:

IF `journald` is the method for capturing logs, all logs of the system should be handled by `journald` and not forwarded to other logging mechanisms.

Audit:

IF `journald` is the method for capturing logs

Review `/etc/systemd/journald.conf` and verify that logs are not forwarded to `rsyslog`.

```
# grep ^\s*ForwardToSyslog /etc/systemd/journald.conf
```

Verify that there is no output.

Remediation:

Edit the `/etc/systemd/journald.conf` file and ensure that `ForwardToSyslog=yes` is removed.

Restart the service:

```
# systemctl restart systemd-journald
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention 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.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

4.1.1.6 Ensure journald log rotation is configured per site policy (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Journald 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/systemd/journald.conf` is the configuration file used to specify how logs generated by Journald should be rotated.

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/systemd/journald.conf` and verify logs are rotated according to site policy. The specific parameters for log rotation are:

```
SystemMaxUse=
SystemKeepFree=
RuntimeMaxUse=
RuntimeKeepFree=
MaxFileSec=
```

Remediation:

Review `/etc/systemd/journald.conf` and verify logs are rotated according to site policy. The settings should be carefully understood as there are specific edge cases and prioritisation of parameters.

The specific parameters for log rotation are:

```
SystemMaxUse=
SystemKeepFree=
RuntimeMaxUse=
RuntimeKeepFree=
MaxFileSec=
```

Additional Information:

See `man 5 journald.conf` for detailed information regarding the parameters in use.

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>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002	TA0040	M1022

4.1.1.7 Ensure journald default file permissions configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Journald 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:

First see if there is an override file `/etc/tmpfiles.d/systemd.conf`. If so, this file will override all default settings as defined in `/usr/lib/tmpfiles.d/systemd.conf` and should be inspected.

If there is no override file, inspect the default `/usr/lib/tmpfiles.d/systemd.conf` against the site specific requirements.

Ensure that file permissions are 0640.

Should a site policy dictate less restrictive permissions, ensure to follow said policy.

NOTE: More restrictive permissions such as 0600 is implicitly sufficient.

Remediation:

If the default configuration is not appropriate for the site specific requirements, copy `/usr/lib/tmpfiles.d/systemd.conf` to `/etc/tmpfiles.d/systemd.conf` and modify as required. Requirements is either 0640 or site policy if that is less restrictive.

Additional Information:

See `man 5 tmpfiles.d` for detailed information on the permission sets for the relevant log files. Further information with examples can be found at
<https://www.freedesktop.org/software/systemd/man/tmpfiles.d.html>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v8	<p>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>5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.</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>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.1.2 Configure rsyslog

The `rsyslog` software package may be used instead of the default `journald` logging mechanism.

Note: This section only applies if `rsyslog` is the chosen method for client side logging. Do not apply this section if `journald` is used.

DRAFT

4.1.2.1 Ensure rsyslog is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsyslog` software is recommended in environments where `journald` does not meet operation requirements.

Rationale:

The security enhancements of `rsyslog` such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

Audit:

Verify `rsyslog` is installed.

Run the following command:

```
# dpkg -s rsyslog | grep "Status:"
```

Verify the output matches:

```
Status: install ok installed
```

Remediation:

Run the following command to install `rsyslog`:

```
# apt install rsyslog
```

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>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000, T1070, T1070.002	TA0005	

4.1.2.2 Ensure rsyslog service is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Once the `rsyslog` package is installed, ensure that the service is enabled.

Rationale:

If the `rsyslog` service is not enabled to start on boot, the system will not capture logging events.

Audit:

Run the following command to verify `rsyslog` is enabled:

```
# systemctl is-enabled rsyslog
```

Verify the output matches:

```
enabled
```

Remediation:

Run the following command to enable `rsyslog`:

```
# systemctl --now enable rsyslog
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.001	TA0005	

4.1.2.3 Ensure journald is configured to send logs to rsyslog (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Data from `journald` may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of `journald` logs, however, use of the RSyslog service provides a consistent means of log collection and export.

Rationale:

IF RSyslog is the preferred method for capturing logs, all logs of the system should be sent to it for further processing.

Audit:

IF RSyslog is the preferred method for capturing logs

Review `/etc/systemd/journald.conf` and verify that logs are forwarded to `rsyslog`.

```
# grep ^\s*ForwardToSyslog /etc/systemd/journald.conf
```

Verify the output matches:

```
ForwardToSyslog=yes
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
ForwardToSyslog=yes
```

Restart the service:

```
# systemctl restart rsyslog
```

Additional Information:

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/journal.conf` is read before any of the custom `*.conf` files. If there are custom configurations present, they override the main configuration parameters

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention 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.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

4.1.2.4 Ensure rsyslog default file permissions are 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.

Impact:

The systems global `umask` could override, but only making the file permissions stricter, what is configured in RSyslog with the `FileCreateMode` directive. RSyslog also has its own `$umask` directive that can alter the intended file creation mode. In addition, consideration should be given to how `FileCreateMode` is used.

Thus it is critical to ensure that the intended file creation mode is not overridden with less restrictive settings in `/etc/rsyslog.conf`, `/etc/rsyslog.d/*conf` files and that `FileCreateMode` is set before any file is created.

Audit:

Run the following command:

```
# grep ^\$FileCreateMode /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Verify the output matches:

```
$FileCreateMode 0640
```

Should a site policy dictate less restrictive permissions, ensure to follow said policy.

NOTE: More restrictive permissions such as 0600 is implicitly sufficient.

Remediation:

Edit either `/etc/rsyslog.conf` or a dedicated `.conf` file in `/etc/rsyslog.d/` and set `$FileCreateMode` to 0640 or more restrictive:

```
$FileCreateMode 0640
```

Restart the service:

```
# systemctl restart rsyslog
```

References:

1. See the `rsyslog.conf(5)` man page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.1.2.5 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 `/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 as expected:

```
# 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.

NOTE: The below configuration is shown for example purposes only. Due care should be given to how the organization wish to store log data.

```
*.emerg                                     :omusrmsg:*
auth,authpriv.*                               /var/log/secure
mail.*                                       -/var/log/mail
mail.info                                     -/var/log/mail.info
mail.warning                                   -/var/log/mail.warn
mail.err                                       /var/log/mail.err
cron.*                                        /var/log/cron
*=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 `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

References:

1. See the `rsyslog.conf(5)` man page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002	TA0005	

4.1.2.6 Ensure rsyslog is configured to send logs to a remote log host (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

RSyslog supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Audit:

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that logs are sent to a central host (where `loghost.example.com` is the name of your central log host):

Old format

```
# grep "^\*\*\*[^I][^I]*@" /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include @@<FQDN or IP of remote loghost>, for example

```
*.* @@loghost.example.com
```

New format

```
# 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>, for example:

```
*.* action(type="omfwd" target="loghost.example.com" port="514" protocol="tcp"
```

Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and add the following line (where `loghost.example.com` is the name of your central log host). The `target` directive may either be a fully qualified domain name or an IP address.

```
*.* action(type="omfwd" target="192.168.2.100" port="514" protocol="tcp"  
        action.resumeRetryCount="100"  
        queue.type="LinkedList" queue.size="1000")
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

References:

1. See the `rsyslog.conf(5)` man page for more information.

Additional Information:

In addition, see the [RSyslog documentation](#) for implementation details of TLS.

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

4.1.2.7 Ensure rsyslog is not configured to receive logs from a remote client (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

RSyslog supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

Rationale:

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside its operational boundary.

Audit:

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that the system is not configured to accept incoming logs.

Old format

```
# grep '$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf  
# grep '$InputTCPServerRun' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

No output expected.

New format

```
# grep -P -- '^h*module\(load="imtcp")' /etc/rsyslog.conf  
/etc/rsyslog.d/*.conf  
# grep -P -- '^h*input\(type="imtcp" port="514")' /etc/rsyslog.conf  
/etc/rsyslog.d/*.conf
```

No output expected.

Remediation:

Should there be any active log server configuration found in the auditing section, modify those file and remove the specific lines highlighted by the audit. Ensure none of the following entries are present in any of `/etc/rsyslog.conf` or `/etc/rsyslog.d/*.conf`.

Old format

```
$ModLoad imtcp  
$InputTCPServerRun
```

New format

```
module(load="imtcp")  
input(type="imtcp" port="514")
```

Restart the service:

```
# systemctl restart rsyslog
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
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>		●	●
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>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0005	

4.1.3 Ensure all logfiles have appropriate permissions and ownership (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Log files contain information from many services on the local system, or in the event of a centralized log server, other systems logs as well. In general log files are found in `/var/log/`, although application can be configured to store logs elsewhere. Should your application store logs in another, ensure to run the same test on that location.

Rationale:

It is important that log files have the correct permissions to ensure that sensitive data is protected and that only the appropriate users / groups have access to them.

Audit:

Run the following script to verify that files in `/var/log/` have appropriate permissions and ownership:

```

#!/usr/bin/env bash

{
    echo -e "\n- Start check - logfiles have appropriate permissions and
ownership"
    output=""
    find /var/log -type f | (while read -r fname; do
        bname=$(basename "$fname")
        case "$bname" in
            lastlog | lastlog.* | wtmp | wtmp.* | btmp | btmp.*)
                if ! stat -Lc "%a" "$fname" | grep -Pq --
'^\h*[0,2,4,6][0,2,4,6][0,4]\h*$'; then
                    output="$output\n- File: \"$fname\" mode: \"$(stat -Lc
"$fname")\"\n"
                fi
                if ! stat -Lc "%U %G" "$fname" | grep -Pq --
'^\h*root\h+(utmp|root)\h*$'; then
                    output="$output\n- File: \"$fname\" ownership: \"$(stat -Lc
"%U:%G" "$fname")\"\n"
                fi
                ;;
            secure | auth.log)
                if ! stat -Lc "%a" "$fname" | grep -Pq --
'^\h*[0,2,4,6][0,4]0\h*$'; then
                    output="$output\n- File: \"$fname\" mode: \"$(stat -Lc "%a"
"$fname")\"\n"
                fi
                if ! stat -Lc "%U %G" "$fname" | grep -Pq --
'^\h*(syslog|root)\h+(adm|root)\h*$'; then
                    output="$output\n- File: \"$fname\" ownership: \"$(stat -Lc
"%U:%G" "$fname")\"\n"
                fi
                ;;
            SSSD | sssd)
                if ! stat -Lc "%a" "$fname" | grep -Pq --
'^\h*[0,2,4,6][0,2,4,6]0\h*$'; then
                    output="$output\n- File: \"$fname\" mode: \"$(stat -Lc "%a"
"$fname")\"\n"
                fi
                if ! stat -Lc "%U %G" "$fname" | grep -Piq --
'^\h*(SSSD|root)\h+(SSSD|root)\h*$'; then
                    output="$output\n- File: \"$fname\" ownership: \"$(stat -Lc
"%U:%G" "$fname")\"\n"
                fi
                ;;
            gdm | gdm3)
                if ! stat -Lc "%a" "$fname" | grep -Pq --
'^\h*[0,2,4,6][0,2,4,6]0\h*$'; then
                    output="$output\n- File: \"$fname\" mode: \"$(stat -Lc "%a"
"$fname")\"\n"
                fi
                if ! stat -Lc "%U %G" "$fname" | grep -Pq --
'^\h*(root)\h+(gdm3?|root)\h*$'; then
                    output="$output\n- File: \"$fname\" ownership: \"$(stat -Lc
"%U:%G" "$fname")\"\n"
                fi
                ;;
        esac
    done
)
}

```

```

        *.journal)
            if ! stat -Lc "%a" "$fname" | grep -Pq --
'^\h*[0,2,4,6][0,4]0\h*$'; then
                output="$output\n- File: \"$fname\" mode: \"$(stat -Lc "%a"
"$fname")\"\n"
            fi
            if ! stat -Lc "%U %G" "$fname" | grep -Pq --
'^\h*(root)\h+(systemd-journal|root)\h*$'; then
                output="$output\n- File: \"$fname\" ownership: \"$(stat -Lc
"%U:%G" "$fname")\"\n"
            fi
            ;;
        *)
            if ! stat -Lc "%a" "$fname" | grep -Pq --
'^\h*[0,2,4,6][0,4]0\h*$'; then
                output="$output\n- File: \"$fname\" mode: \"$(stat -Lc "%a"
"$fname")\"\n"
            fi
            if ! stat -Lc "%U %G" "$fname" | grep -Pq --
'^\h*(syslog|root)\h+(adm|root)\h*$'; then
                output="$output\n- File: \"$fname\" ownership: \"$(stat -Lc
"%U:%G" "$fname")\"\n"
            fi
            ;;
        esac
    done
    # If all files passed, then we pass
    if [ -z "$output" ]; then
        echo -e "\n- PASS\n- All files in \"/var/log/\" have appropriate
permissions and ownership\n"
    else
        # print the reason why we are failing
        echo -e "\n- FAIL:\n$output"
    fi
    echo -e "- End check - logfiles have appropriate permissions and
ownership\n"
)
}

```

Remediation:

Run the following script to update permissions and ownership on files in `/var/log`. Although the script is not destructive, ensure that the output of the audit procedure is captured in the event that the remediation causes issues.

```

#!/usr/bin/env bash

{
    echo -e "\n- Start remediation - logfiles have appropriate permissions and
ownership"
    find /var/log -type f | while read -r fname; do
        bname=$(basename "$fname")
        case "$bname" in
            lastlog | lastlog.* | wtmp | wtmp.* | btmp | btmp.*)
                ! stat -Lc "%a" "$fname" | grep -Pq --
'^\h*[0,2,4,6][0,2,4,6][0,4]\h*$' && echo -e "- changing mode on \"$fname\""
&& chmod ug-x,o-wx "$fname"
                ! stat -Lc "%U" "$fname" | grep -Pq -- '^h*root\h*$' && echo -e
"- changing owner on \"$fname\"" && chown root "$fname"
                ! stat -Lc "%G" "$fname" | grep -Pq -- '^h*(utmp|root)\h*$' &&
echo -e "- changing group on \"$fname\"" && chgrp root "$fname"
            ;;
            secure | auth.log)
                ! stat -Lc "%a" "$fname" | grep -Pq -- '^h*[0,2,4,6][0,4]0\h*$'
&& echo -e "- changing mode on \"$fname\"" && chmod u-x,g-wx,o-rwx "$fname"
                ! stat -Lc "%U" "$fname" | grep -Pq -- '^h*(syslog|root)\h*$' &&
echo -e "- changing owner on \"$fname\"" && chown root "$fname"
                ! stat -Lc "%G" "$fname" | grep -Pq -- '^h*(adm|root)\h*$' &&
echo -e "- changing group on \"$fname\"" && chgrp root "$fname"
            ;;
            SSSD | sssd)
                ! stat -Lc "%a" "$fname" | grep -Pq --
'^\h*[0,2,4,6][0,2,4,6]0\h*$' && echo -e "- changing mode on \"$fname\"" &&
chmod ug-x,o-rwx "$fname"
                ! stat -Lc "%U" "$fname" | grep -Piq -- '^h*(SSSD|root)\h*$' &&
echo -e "- changing owner on \"$fname\"" && chown root "$fname"
                ! stat -Lc "%G" "$fname" | grep -Piq -- '^h*(SSSD|root)\h*$' &&
echo -e "- changing group on \"$fname\"" && chgrp root "$fname"
            ;;
            gdm | gdm3)
                ! stat -Lc "%a" "$fname" | grep -Pq --
'^\h*[0,2,4,6][0,2,4,6]0\h*$' && echo -e "- changing mode on \"$fname\"" &&
chmod ug-x,o-rwx
                ! stat -Lc "%U" "$fname" | grep -Pq -- '^h*root\h*$' && echo -e
"- changing owner on \"$fname\"" && chown root "$fname"
                ! stat -Lc "%G" "$fname" | grep -Pq -- '^h*(gdm3?|root)\h*$' &&
echo -e "- changing group on \"$fname\"" && chgrp root "$fname"
            ;;
            *.journal)
                ! stat -Lc "%a" "$fname" | grep -Pq -- '^h*[0,2,4,6][0,4]0\h*$'
&& echo -e "- changing mode on \"$fname\"" && chmod u-x,g-wx,o-rwx "$fname"
                ! stat -Lc "%U" "$fname" | grep -Pq -- '^h*root\h*$' && echo -e
"- changing owner on \"$fname\"" && chown root "$fname"
                ! stat -Lc "%G" "$fname" | grep -Pq -- '^h*(systemd-
journal|root)\h*$' && echo -e "- changing group on \"$fname\"" && chgrp root
"$fname"
            ;;
        *)
                ! stat -Lc "%a" "$fname" | grep -Pq -- '^h*[0,2,4,6][0,4]0\h*$'
&& echo -e "- changing mode on \"$fname\"" && chmod u-x,g-wx,o-rwx "$fname"
                ! stat -Lc "%U" "$fname" | grep -Pq -- '^h*(syslog|root)\h*$' &&
echo -e "- changing owner on \"$fname\"" && chown root "$fname"
        ;;
    esac
}

```

```

        ! stat -Lc "%G" "$fname" | grep -Pq -- '^\\h*(adm|root)\\h*$' &&
echo -e "-- changing group on \\\"$fname\\\" && chgrp root "$fname"
;;
esac
done
echo -e "- End remediation - logfiles have appropriate permissions and
ownership\\n"
}

```

Note: You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.

If there are services that log to other locations, ensure that those log files have the appropriate permissions.

Additional Information:

NIST SP 800-53 Rev. 5:

- AC-3
- MP-2

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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.2 Configure System Accounting (auditd)

The Linux Auditing System operates on a set of rules that collects certain types of system activity to facilitate incident investigation, detect unauthorized access or modification of data. By default events will be logged to `/var/log/audit/audit.log`, which can be configured in `/etc/audit/auditd.conf`.

The following types of audit rules can be specified:

- Control rules: Configuration of the auditing system.
- File system rules: Allow the auditing of access to a particular file or a directory. Also known as file watches.
- System call rules: Allow logging of system calls that any specified program makes.

Audit rules can be set:

- On the command line using the `auditctl` utility. These rules are not persistent across reboots.
- In `/etc/audit/audit.rules`. These rules have to be merged and loaded before they are active.

Notes:

- For 64 bit systems that have `arch` as a rule parameter, you will need two rules: one for 64 bit and one for 32 bit systems calls. For 32 bit systems, only one rule is needed.
- If the auditing system is configured to be locked (`-e 2`), a system reboot will be required in order to load any changes.
- Key names are optional on the rules and will not be used as a compliance auditing. The usage of key names is highly recommended as it facilitates organisation and searching, as such, all remediation steps will have key names supplied.
- It is best practice to store the rules, in number prepended files, in `/etc/audit/rules.d/`. Rules must end in a `.rules` suffix. This then requires the use of `augenrules` to merge all the rules into `/etc/audit/audit.rules` based on their their alphabetical (lexical) sort order. All benchmark recommendations follow this best practice for remediation, specifically using the prefix of 50 which is centre weighed if all rule sets make use of the number prepending naming convention.
- Your system may have been customized to change the default `UID_MIN`. All samples output uses 1000, but this value will not be used in compliance auditing. To confirm the `UID_MIN` for your system, run the following command: `awk '/^s*UID_MIN/{print $2}' /etc/login.defs`

Normalization

The Audit system normalizes some entries, so when you look at the sample output keep in mind that:

- With regards to users whose login UID is not set, the values `-1` / `unset` / `4294967295` are equivalent and normalized to `-1`.
- When comparing field types and both sides of the comparison is valid fields types, such as `euid!=uid`, then the auditing system may normalize such that the output is `uid!=euid`.
- Some parts of the rule may be rearranged whilst others are dependant on previous syntax. For example, the following two statements are the same:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F auid!=-1 -F  
key=user_emulation
```

and

```
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k  
user_emulation
```

Capacity planning

The recommendations in this section implement auditing policies that not only produces large quantities of logged data, but may also negatively impact system performance. Capacity planning is critical in order not to adversely impact production environments.

- Disk space. If a significantly large set of events are captured, additional on system or off system storage may need to be allocated. If the logs are not sent to a remote log server, ensure that log rotation is implemented else the disk will fill up and the system will halt. Even when logs are sent to a log server, ensure sufficient disk space to allow caching of logs in the case of temporary network outages.
- Disk IO. It is not just the amount of data collected that should be considered, but the rate at which logs are generated.
- CPU overhead. System call rules might incur considerable CPU overhead. Test the systems open/close syscalls per second with and without the rules to gauge the impact of the rules.

4.2.1 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.

DRAFT

4.2.1.1 Ensure auditd is installed (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - 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 and audispd-plugins are installed:

```
# dpkg -s auditd audispd-plugins | grep -E '(Package:|Status|not installed)'  
  
Package: auditd  
Status: install ok installed  
Package: audispd-plugins  
Status: install ok installed
```

Remediation:

Run the following command to Install auditd

```
# apt install auditd audispd-plugins and audispd-plugins
```

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>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	

4.2.1.2 Ensure auditd service is enabled and active (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Turn on the `auditd` daemon to record system events.

Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Audit:

Run the following command to verify `auditd` is enabled:

```
# systemctl is-enabled auditd  
enabled
```

Verify result is "enabled".

Run the following command to verify `auditd` is active:

```
# systemctl is-active auditd  
active
```

Verify result is active

Remediation:

Run the following command to enable and start `auditd`:

```
# systemctl --now enable auditd
```

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	

4.2.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Configure `grub2` so that processes that are capable of being audited can be audited even if they start up prior to `auditd` startup.

Rationale:

Audit events need to be captured on processes that start up prior to `auditd`, so that potential malicious activity cannot go undetected.

Audit:

Run the following command:

```
# find /boot -type f -name 'grub.cfg' -exec grep -Ph -- '^\\h*linux' {} + | grep -v 'audit=1'
```

Nothing should be returned.

Remediation:

Edit `/etc/default/grub` and add `audit=1` to `GRUB_CMDLINE_LINUX`:

Example:

```
GRUB_CMDLINE_LINUX="audit=1"
```

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

```
# update-grub
```

Additional Information:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	

4.2.1.4 Ensure audit_backlog_limit is sufficient (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

In the kernel-level audit subsystem, a socket buffer queue is used to hold audit events. Whenever a new audit event is received, it is logged and prepared to be added to this queue.

The kernel boot parameter `audit_backlog_limit=N`, with `N` representing the amount of messages, will ensure that a queue cannot grow beyond a certain size. If an audit event is logged which would grow the queue beyond this limit, then a failure occurs and is handled according to the system configuration

Rationale:

If an audit event is logged which would grow the queue beyond the `audit_backlog_limit`, then a failure occurs, auditd records will be lost, and potential malicious activity could go undetected.

Audit:

Run the following command and verify the `audit_backlog_limit=` parameter is set:

```
# find /boot -type f -name 'grub.cfg' -exec grep -Ph -- '^h*linux' {} + | grep -Pv 'audit_backlog_limit=\d+\b'
```

Nothing should be returned.

Remediation:

Edit `/etc/default/grub` and add `audit_backlog_limit=N` to `GRUB_CMDLINE_LINUX`. The recommended size for `N` is 8192 or larger.

Example:

```
GRUB_CMDLINE_LINUX="audit_backlog_limit=8192"
```

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

```
# update-grub
```

Default Value:

if `audit_backlog_limit` is not set, the system defaults to `audit_backlog_limit=64`

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>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	

4.2.2 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.

DRAFT

4.2.2.1 Ensure audit log storage size is configured (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.

Rationale:

It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

Audit:

Run the following command and ensure output is in compliance with site policy:

```
# grep -Po -- '^h*max_log_file\h*=\h*\d+\b' /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>
```

Default Value:

```
max_log_file = 8
```

Additional Information:

The `max_log_file` parameter is measured in megabytes.

Other methods of log rotation may be appropriate based on site policy. One example is time-based rotation strategies which don't have native support in auditd configurations. Manual audit of custom configurations should be evaluated for effectiveness and completeness.

CIS Controls:

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0040	M1053

4.2.2.2 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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1053

4.2.2.3 Ensure system is disabled when audit logs are full (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `auditd` daemon can be configured to halt the system when the audit logs are full.

The `admin_space_left_action` parameter tells the system what action to take when the system has detected that it is low on disk space. Valid values are `ignore`, `syslog`, `suspend`, `single`, and `halt`.

- `ignore`, the audit daemon does nothing
- `Syslog`, the audit daemon will issue a warning to syslog
- `Suspend`, the audit daemon will stop writing records to the disk
- `single`, the audit daemon will put the computer system in single user mode
- `halt`, the audit daemon will shutdown the system

Rationale:

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

Impact:

If the `admin_space_left_action` parameter is set to `halt` the audit daemon will shutdown the system when the disk partition containing the audit logs becomes full.

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
```

Run the following command and verify the output is either halt **or** single:

```
# grep -E 'admin_space_left_action\s*=\s*(halt|single)'  
/etc/audit/auditd.conf  
  
admin_space_left_action = <halt|single>
```

Remediation:

Set the following parameters in /etc/audit/auditd.conf:

```
space_left_action = email  
action_mail_acct = root
```

set admin_space_left_action to either halt **or** single in /etc/audit/auditd.conf.

Example:

```
admin_space_left_action = halt
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	

4.2.3 Configure auditd rules

The Audit system operates on a set of rules that define what is to be captured in the log files.

The following types of Audit rules can be specified:

- Control rules: Allow the Audit system's behavior and some of its configuration to be modified.
- File system rules: Allow the auditing of access to a particular file or a directory. (Also known as file watches)
- System call rules: Allow logging of system calls that any specified program makes.

Audit rules can be set:

- on the command line using the `auditctl` utility. Note that these rules are not persistent across reboots.
- in a file ending in `.rules` in the `/etc/audit/audit.d/` directory.

4.2.3.1 Ensure changes to system administration scope (`sudoers`) is collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor scope changes for system administrators. If the system has been properly configured to force system administrators to log in as themselves first and then use the `sudo` command to execute privileged commands, it is possible to monitor changes in scope. The file `/etc/sudoers`, or files in `/etc/sudoers.d`, will be written to when the file(s) or related attributes have changed. The audit records will be tagged with the identifier "scope".

Rationale:

Changes in the `/etc/sudoers` and `/etc/sudoers.d` files can indicate that an unauthorized change has been made to the scope of system administrator activity.

Audit:

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&!/etc\sudoers/ \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&!/etc\sudoers/ \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor scope changes for system administrators.

Example:

```
# printf "
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
" >> /etc/audit/rules.d/50-scope.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>4.8 Log and Alert on Changes to Administrative Group Membership</p> <p>Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0004	M1047

4.2.3.2 Ensure actions as another user are always logged (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

`sudo` provides users with temporary elevated privileges to perform operations, either as the superuser or another user.

Rationale:

Creating an audit log of users 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`'s logfile to verify if unauthorized commands have been executed.

Audit:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-a always,exit/ \
&& -F arch=b(32|64) / \
&&(/ -F auid!=unset/||/ -F auid!=-1/||/ -F auid!=4294967295/) \
&&(/ -C euid!=uid/||/ -C uid!=euid/) \
&&/ -S execve/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/) ' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
-a always,exit -F arch=b32 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-a always,exit/ \
&& -F arch=b(32|64) / \
&&(/ -F auid!=unset/||/ -F auid!=-1/||/ -F auid!=4294967295/) \
&&(/ -C euid!=uid/||/ -C uid!=euid/) \
&&/ -S execve/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/) '
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F auid==-1 -F
key=user_emulation
-a always,exit -F arch=b32 -S execve -C uid!=euid -F auid==-1 -F
key=user_emulation
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor elevated privileges.

64 Bit systems

Example:

```
# printf "
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
-a always,exit -F arch=b32 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
" >> /etc/audit/rules.d/50-user_emulation.rules
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.</p>		●	●
v7	<p>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>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0004	M1047

4.2.3.3 Ensure events that modify the sudo log file are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor the `sudo` log file. If the system has been properly configured to disable the use of the `su` command and force all administrators to have to log in first and then use `sudo` to execute privileged commands, then all administrator commands will be logged to `/var/log/sudo.log`. Any time a command is executed, an audit event will be triggered as the `/var/log/sudo.log` file will be opened for write and the executed administration command will be written to the log.

Rationale:

Changes in `/var/log/sudo.log` indicate that an administrator has executed a command or the log file itself has been tampered with. Administrators will want to correlate the events written to the audit trail with the records written to `/var/log/sudo.log` to verify if unauthorized commands have been executed.

Impact:

NOTE: The section *Configure sudo* must be completed first. Not all distributions install `sudo` by default, nor does the default configuration after installation necessarily have the `logfile` parameter which is required for this audit.

Audit:

On disk configuration

Run the following command to check the on disk rules:

```
# SUDO_LOG_FILE_ESCAPED=$(grep -r logfile /etc/sudoers* | sed -e  
's/.*logfile=//;s/,? .*/' -e 's///g' -e 's|/|\\/|g')  
# [ -n "${SUDO_LOG_FILE_ESCAPED}" ] && awk "/^ *-w/ \  
&&/"${SUDO_LOG_FILE_ESCAPED}"/ \  
&&/ +p *wa/ \  
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \  
|| printf "ERROR: Variable 'SUDO_LOG_FILE_ESCAPED' is unset.\n"
```

Verify output of matches:

```
-w /var/log/sudo.log -p wa -k sudo_log_file
```

Running configuration

Run the following command to check loaded rules:

```
# SUDO_LOG_FILE_ESCAPED=$(grep -r logfile /etc/sudoers* | sed -e  
's/.*logfile=//;s/,? .*/' -e 's///g' -e 's|/|\\/|g')  
# [ -n "${SUDO_LOG_FILE_ESCAPED}" ] && auditctl -l | awk "/^ *-w/ \  
&&/"${SUDO_LOG_FILE_ESCAPED}"/ \  
&&/ +p *wa/ \  
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" \  
|| printf "ERROR: Variable 'SUDO_LOG_FILE_ESCAPED' is unset.\n"
```

Verify output matches:

```
-w /var/log/sudo.log -p wa -k sudo_log_file
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the sudo log file.

Example:

```
# SUDO_LOG_FILE=$(grep -r logfile /etc/sudoers* | sed -e 's/.*/logfile=//;s/,? .*/' -e 's/"//g')
# [ -n "${SUDO_LOG_FILE_ESCAPED}" ] && printf "
-w ${SUDO_LOG_FILE} -p wa -k sudo_log_file
" >> /etc/audit/rules.d/50-sudo.rules \
|| printf "ERROR: Variable 'SUDO_LOG_FILE_ESCAPED' is unset.\n"
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>4.9 Log and Alert on Unsuccessful Administrative Account Login</u> Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●

4.2.3.4 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
- `clock_gettime` - allows for the setting of several internal clocks and timers

system calls have been executed. Further, ensure to write an audit record to the configured audit log file upon exit, tagging the records with a unique identifier such as "time-change".

Rationale:

Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Audit:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-a *always,exit/ \
&& / -F *arch=b(32|64)/ \
&& / -S/ \
&& (/adjtimex/ \
||/settimeofday/ \
||/clock_gettime/ ) \
&& (/ key= *[!-~]* *$||/ -k *[!-~]* *$/) ' /etc/audit/rules.d/*.rules

# awk '/^ *-w/ \
&& /etc/localtime/ \
&& +-p *wa/ \
&& (/ key= *[!-~]* *$||/ -k *[!-~]* *$/) ' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -k time-change
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-a *always,exit/ \
&& -F arch=b(32|64) / \
&& -S / \
&& (/adjtimex/ \
||/settimeofday/ \
||/clock_settime/ ) \
&& (/ key= *[!-~]* *$||/ -k *[!-~]* *$/)'

# auditctl -l | awk '/^ *-w/ \
&& /etc/localtime/ \
&& +-p wa/ \
&& (/ key= *[!-~]* *$||/ -k *[!-~]* *$/)'
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -F
key=time-change
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime -F
key=time-change
-w /etc/localtime -p wa -k time-change
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.
In addition, also audit for the stime system call rule. For example:

```
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime,stime -k
time-change
```

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify date and time information.

64 Bit systems

Example:

```
# printf "
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -k time-
change
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime -k time-
change
-w /etc/localtime -p wa -k time-change
" >> /etc/audit/rules.d/50-time-change.rules
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`. In addition, add `stime` to the system call audit. Example:

```
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime,stime -k
time-change
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	

4.2.3.5 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 monitors the following system calls, and write an audit event on system call exit:

- `sethostname` - set the systems host name
- `setdomainname` - set the systems domain name

The files being monitored are:

- `/etc/issue` and `/etc/issue.net` - messages displayed pre-login
- `/etc/hosts` - file containing host names and associated IP addresses
- `/etc/networks` - symbolic names for networks
- `/etc/network/` - directory containing network interface scripts and configurations files

Rationale:

Monitoring `sethostname` and `setdomainname` will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The `/etc/hosts` file is monitored for changes 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 should have a relevant tag associated with them.

Audit:

64 Bit systems

On disk configuration

Run the following commands to check the on disk rules:

```

# awk '/^ *-a *always,exit/ \
&& / -F arch=b(32|64)/ \
&& / -S/ \
&& (/sethostname/ \
||/setdomainname/) \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules

# awk '/^ *-w/ \
&&(/etc/issue/ \
||/etc/issue.net/ \
||/etc/hosts/ \
||/etc/network/) \
&& / +p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules

```

Verify the output matches:

```

-a always,exit -F arch=b64 -S sethostname,setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname,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/networks -p wa -k system-locale
-w /etc/network/ -p wa -k system-locale

```

Running configuration

Run the following command to check loaded rules:

```

# auditctl -l | awk '/^ *-a *always,exit/ \
&& / -F arch=b(32|64)/ \
&& / -S/ \
&& (/sethostname/ \
||/setdomainname/) \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' 

# auditctl -l | awk '/^ *-w/ \
&&(/etc/issue/ \
||/etc/issue.net/ \
||/etc/hosts/ \
||/etc/network/) \
&& / +p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'

```

Verify the output includes:

```

-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/networks -p wa -k system-locale
-w /etc/network/ -p wa -k system-locale

```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the system's network environment.

64 Bit systems

Example:

```
# printf "
-a always,exit -F arch=b64 -S sethostname,setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname,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/networks -p wa -k system-locale
-w /etc/network/ -p wa -k system-locale
" >> /etc/audit/rules.d/50-system_local.rules
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>5.5 Implement Automated Configuration Monitoring Systems</p> <p>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>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0003	M1047

4.2.3.6 Ensure use of privileged commands are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor privileged programs, those that have the `setuid` and/or `setgid` bit set on execution, to determine if unprivileged users are running these commands.

Rationale:

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

Impact:

Both the audit and remediation section of this recommendation will traverse all mounted file systems that is not mounted with either `noexec` or `nosuid` mount options. If there are large file systems without these mount options, **such traversal will be significantly detrimental to the performance of the system.**

Before running either the audit or remediation section, inspect the output of the following command to determine exactly which file systems will be traversed:

```
# findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid"
```

To exclude a particular file system due to adverse performance impacts, update the audit and remediation sections by adding a sufficiently unique string to the `grep` statement. The above command can be used to test the modified exclusions.

Audit:

On disk configuration

Run the following command to check on disk rules:

```
# for PARTITION in $(findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid" | awk '{print $1}'); do
    for PRIVILEGED in $(find "${PARTITION}" -xdev -perm /6000 -type f); do
        grep -qr "${PRIVILEGED}" /etc/audit/rules.d && printf "OK:
'${PRIVILEGED}' found in auditing rules.\n" || printf "Warning:
'${PRIVILEGED}' not found in on disk configuration.\n"
    done
done
```

Verify that all output is OK.

Running configuration

Run the following command to check loaded rules:

```
# RUNNING=$(auditctl -l)
# [ -n "${RUNNING}" ] && for PARTITION in $(findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid" | awk '{print $1}'); do
    for PRIVILEGED in $(find "${PARTITION}" -xdev -perm /6000 -type f); do
        printf -- "${RUNNING}" | grep -q "${PRIVILEGED}" && printf "OK:
'${PRIVILEGED}' found in auditing rules.\n" || printf "Warning:
'${PRIVILEGED}' not found in running configuration.\n"
    done
done \
|| printf "ERROR: Variable 'RUNNING' is unset.\n"
```

Verify that all output is OK.

Special mount points

If there are any special mount points that are not visible by default from `findmnt` as per the above audit, said file systems would have to be manually audited.

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor the use of privileged commands.

Example:

```
# build_audit_rules()
(
    UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
    AUDIT_RULE_FILE="/etc/audit/rules.d/50-privileged.rules"
    NEW_DATA=()
    for PARTITION in $(findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid" | awk '{print $1}'); do
        readarray -t DATA < <(find "${PARTITION}" -xdev -perm /6000 -type f | awk -v UID_MIN=${UID_MIN} '{print "-a always,exit -F path=\"\$1\" -F perm=x -F auid>=\"UID_MIN\" -F auid!=unset -k privileged"}')
        for ENTRY in "${DATA[@]}"; do
            NEW_DATA+=("{$ENTRY}")
        done
    done
    readarray &> /dev/null -t OLD_DATA < "${AUDIT_RULE_FILE}"
    COMBINED_DATA=( "${OLD_DATA[@]}" "${NEW_DATA[@]}" )
    printf '%s\n' "${COMBINED_DATA[@]}" | sort -u > "${AUDIT_RULE_FILE}"
)
build_audit_rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

Special mount points

If there are any special mount points that are not visible by default from just scanning `/`, change the `PARTITION` variable to the appropriate partition and re-run the remediation.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0002	M1026

4.2.3.7 Ensure unsuccessful file access attempts are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor for unsuccessful attempts to access files. The following parameters are associated with system calls that control files:

- creation - `creat`
- opening - `open` , `openat`
- truncation - `truncate` , `ftruncate`

An audit log record will only be written if all of the following criteria is met for the user when trying to access a file:

- a non-privileged user (`auid>=UID_MIN`)
- is not a Daemon event (`auid=4294967295/unset/-1`)
- if the system call returned EACCES (permission denied) or EPERM (some other permanent error associated with the specific system call)

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:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```

# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&(/ -F *exit=-EACCES/||/ -F *exit=-EPERM/) \
&&/ -S/ \
&&/creat/ \
&&/open/ \
&&/truncate/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/) " /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"

```

Verify the output includes:

```

-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=unset -k access
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=unset -k access

```

Running configuration

Run the following command to check loaded rules:

```

# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&(/ -F *exit=-EACCES/||/ -F *exit=-EPERM/) \
&&/ -S/ \
&&/creat/ \
&&/open/ \
&&/truncate/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/) \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"

```

Verify the output includes:

```

-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=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,truncate,ftruncate,creat,openat -F exit=-EACCES -F auid>=1000 -F auid!=-1 -F key=access
-a always,exit -F arch=b32 -S open,truncate,ftruncate,creat,openat -F exit=-EPERM -F auid>=1000 -F auid!=-1 -F key=access

```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

Remediation:

For 32 bit systems edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor unsuccessful file access attempts.

64 Bit systems

Example:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit==EACCES -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit==EPERM -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit==EACCES -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit==EPERM -F auid>=${UID_MIN} -F auid!=unset -k access
" >> /etc/audit/rules.d/50-access.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (-e 2), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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).			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0007	

4.2.3.8 Ensure events that modify user/group information are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Record events affecting the modification of user or group information, including that of passwords and old passwords if in use.

- /etc/group - system groups
- /etc/passwd - system users
- /etc/gshadow - encrypted password for each group
- /etc/shadow - system user passwords
- /etc/security/opasswd - storage of old passwords if the relevant PAM module is in use

The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier "identity" in the audit log file.

Rationale:

Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Audit:

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/etc/group/ \
||/etc/passwd/ \
||/etc/gshadow/ \
||/etc/shadow/ \
||/etc/security/opasswd/) \
&& / +p *wa/ \
&&(/ key= *[!-~]* *$/ ||/ -k *[!-~]* *$/)' /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
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/etc/group/ \
||/etc/passwd/ \
||/etc/gshadow/ \
||/etc/shadow/ \
||/etc/security/opasswd/) \
&& / +p *wa/ \
&&(/ key= *[!-~]* *$/ ||/ -k *[!-~]* *$/)'
```

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` extension, with the relevant rules to monitor events that modify user/group information.

Example:

```
# printf "
-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
" >> /etc/audit/rules.d/50-identity.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0004	M1047

4.2.3.9 Ensure discretionary access control permission modification events are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The following commands and system calls effect the permissions, ownership and various attributes of files.

- chmod
- fchmod
- fchmodat
- chown
- fchown
- fchownat
- lchown
- setxattr
- lsetxattr
- fsetxattr
- removexattr
- lremovexattr
- fremovexattr

In all cases, an audit record will only be written for non-system user ids and will ignore Daemon events. All audit records will be tagged with the identifier "perm_mod."

Rationale:

Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Audit:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&& / -F *arch=b(32|64)/ \
&& / -F *auid!=unset/ ||| -F *auid!=-1/ ||| -F *auid!=4294967295/) \
&& / -S/ \
&& / -F *auid>=${UID_MIN}/ \
&& (/chmod/|||fchmod/|||fchmodat/ \
|||chown/|||fchown/|||fchownat/|||lchown/ \
|||setxattr/|||lsetxattr/|||fsetxattr/ \
|||removexattr/|||lremovexattr/|||fremovexattr/) \
&& (/ key= *[!~]* *$/||| -k *[!~]* *$/) " /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=unset -F key=perm_mod
```

Running configuration

Run the following command to check loaded rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&& / -F *arch=b(32|64)/ \
&& / -F *auid!=unset/ ||| -F *auid!=-1/ ||| -F *auid!=4294967295/) \
&& / -S/ \
&& / -F *auid>=${UID_MIN}/ \
&& (/chmod/|||fchmod/|||fchmodat/ \
|||chown/|||fchown/|||fchownat/|||lchown/ \
|||setxattr/|||lsetxattr/|||fsetxattr/ \
|||removexattr/|||lremovexattr/|||fremovexattr/) \
&& (/ key= *[!~]* *$/||| -k *[!~]* *$/) \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the 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=b64 -S chown,fchown,lchown,fchownat -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=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
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor discretionary access control permission modification events.

64 Bit systems

Example:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=${UID_MIN} -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=${UID_MIN} -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
" >> /etc/audit/rules.d/50-perm_mod.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (-e 2), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1022

4.2.3.10 Ensure successful file system mounts are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor the use of the `mount` system call. The `mount` (and `umount`) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the `mount` system call is used by a non-privileged user

Rationale:

It is highly unusual for a non privileged user to `mount` file systems to the system. While tracking `mount` commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful `open`, `creat` and `truncate` system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

Audit:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -S/ \
&&/mount/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/) " /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -k mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -k mounts
```

Running configuration

Run the following command to check loaded rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -S/ \
&&/mount/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/) \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the 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
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful file system mounts.

64 Bit systems

Example:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -k mounts
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -k mounts
" >> /etc/audit/rules.d/50-perm_mod.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0010	M1034

4.2.3.11 Ensure session initiation information is collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor session initiation events. The parameters in this section track changes to the files associated with session events.

- `/var/run/utmp` - tracks all currently logged in users.
- `/var/log/wtmp` - file tracks logins, logouts, shutdown, and reboot events.
- `/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 "session."

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:

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/\/var\/run\/utmp/ \
||/\/var\/log\/wtmp/ \
||/\/var\/log\/btmp/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/ ||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/\/var\/run\/utmp/ \
||/\/var\/log\/wtmp/ \
||/\/var\/log\/btmp/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/ ||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor session initiation information.

Example:

```
# printf "
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
" >> /etc/audit/rules.d/50-session.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.</p>		●	●
v7	<p>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>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>			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0001	

4.2.3.12 Ensure login and logout events are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor login and logout events. The parameters below track changes to files associated with login/logout events.

- `/var/log/lastlog` - maintain records of the last time a user successfully logged in.
- `/var/run/faillock` - directory maintains records of login failures via the `pam_faillock` module.

Rationale:

Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Audit:

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/var/log/lastlog/ \
||/var/run/faillock/) \
&&/ +p *wa/ \
&&(/ key= *[!~]* *$/ ||/ -k *[!~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/var/log/lastlog/ \
||/var/run/faillock/) \
&&/ +p *wa/ \
&&(/ key= *[!~]* *$/ ||/ -k *[!~]* *$/)'
```

Verify the output matches:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor login and logout events.

Example:

```
# printf "
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
" >> /etc/audit/rules.d/50-login.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.</p>		●	●
v7	<p>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>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>			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0001	

4.2.3.13 Ensure file deletion events by users are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for:

- `unlink` - remove a file
- `unlinkat` - remove a file attribute
- `rename` - rename a file
- `renameat` rename a file attribute system calls and tags them with the identifier "delete".

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:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&& / -F *arch=b(32|64)/ \
&& / -F *auid!=unset/ || / -F *auid!=-1/ || / -F *auid!=4294967295/ ) \
&& / -F *auid>=${UID_MIN}/ \
&& / -S/ \
&& (/unlink/||/rename/||/unlinkat/||/renameat/) \
&& (/ key= *[^-~]* *$/|| / -k *[^-~]* *$/) " /etc/audit/rules.d/*.*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat -F auid>=1000 -
F auid!=unset -k delete
-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat -F auid>=1000 -
F auid!=unset -k delete
```

Running configuration

Run the following command to check loaded rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&& / -F *arch=b(32|64)/ \
&& / -F *auid!=unset/ || / -F *auid!=-1/ || / -F *auid!=4294967295/ ) \
&& / -F *auid>=${UID_MIN}/ \
&& / -S/ \
&& (/unlink/||/rename/||/unlinkat/||/renameat/) \
&& (/ key= *[^-~]* *$/|| / -k *[^-~]* *$/) " \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the 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
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor file deletion events by users.

64 Bit systems

Example:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F
auid>=${UID_MIN} -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S rename,unlink,unlinkat,renameat -F
auid>=${UID_MIN} -F auid!=unset -F key=delete
" >> /etc/audit/rules.d/50-delete.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	13 <u>Data Protection</u> Data Protection			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	

4.2.3.14 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor AppArmor, an implementation of mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the `/etc/apparmor/` and `/etc/apparmor.d/` directories.

Note: If a different Mandatory Access Control method is used, changes to the corresponding directories should be audited.

Rationale:

Changes to files in the `/etc/apparmor/` and `/etc/apparmor.d/` 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:

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/etc/apparmor/ \
||/etc/apparmor.d/) \
&& / +p *wa/ \
&&(/ key= *[!-~]* *$/ ||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/etc/apparmor/ \
||/etc/apparmor.d/) \
&& / +p *wa/ \
&&(/ key= *[!-~]* *$/ ||/ -k *[!-~]* *$/)'
```

Verify the 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` extension, with the relevant rules to monitor events that modify the system's Mandatory Access Controls.

Example:

```
# printf "
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
" >> /etc/audit/rules.d/50-MAC-policy.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.</p>		●	●
v7	<p>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>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0004	M1022

4.2.3.15 Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - 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:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/chcon/ \
&&(/ key= *[!~]* *$/||/ -k *[!~]* *$/) /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset
-k perm_chng
```

Running configuration

Run the following command to check loaded rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/chcon/ \
&&(/ key= *[!~]* *$/||/ -k *[!~]* *$/) \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_chng
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `chcon` command.

64 Bit systems

Example:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && printf "
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-perm_chng.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

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.	●	●	●

4.2.3.16 Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - 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:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/setfacl/ \
&&(/ key= *[!~]* *$/||/ -k *[!~]* *$/) /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=unset -k perm_chng
```

Running configuration

Run the following command to check loaded rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/setfacl/ \
&&(/ key= *[!~]* *$/||/ -k *[!~]* *$/) \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_chng
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `setfacl` command.

64 Bit systems

Example:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && printf "
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-priv_cmd.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

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.	●	●	●

4.2.3.17 Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - 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:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/chacl/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/) /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=unset
-k priv_cmd
```

Running configuration

Run the following command to check loaded rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/chacl/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/) \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F
auid!=-1 -F key=priv_cmd
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `chacl` command.

64 Bit systems

Example:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "$UID_MIN" ] && printf "
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-perm_chng.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

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.	●	●	●

4.2.3.18 Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - 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:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/sbin/usermod/ \
&&(/ key= *[!~]* *$/||/ -k *[!~]* *$/) /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the output matches:

```
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=unset -k usermod
```

Running configuration

Run the following command to check loaded rules:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/sbin/usermod/ \
&&(/ key= *[!~]* *$/||/ -k *[!~]* *$/) \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=-1 -F key=usermod
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `usermod` command.

64 Bit systems

Example:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && printf "
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k usermod
" >> /etc/audit/rules.d/50-usermod.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

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.	●	●	●

4.2.3.19 Ensure kernel module loading unloading and modification is collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor the loading and unloading of kernel modules. All the loading / listing / dependency checking of modules is done by `kmod` via symbolic links.

The following system calls control loading and unloading of modules:

- `init_module` - load a module
- `finit_module` - load a module (used when the overhead of using cryptographically signed modules to determine the authenticity of a module can be avoided)
- `delete_module` - delete a module
- `create_module` - create a loadable module entry
- `query_module` - query the kernel for various bits pertaining to modules

Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of `modules`.

Rationale:

Monitoring the use of all the various ways to manipulate kernel modules could provide system administrators with evidence that an unauthorized change was made to a kernel module, possibly compromising the security of the system.

Audit:

64 Bit systems

On disk configuration

Run the following commands to check the on disk rules:

```
# awk '/^ *-a always,exit/ \
&& -F arch=b(32|64) / \
&&(/ -F auid!=unset/||/ -F auid==1/||/ -F auid!=4294967295/) \
&& -S/ \
&&(/init_module/ \
||/finit_module/ \
||/delete_module/ \
||/create_module/ \
||/query_module/) \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules

# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && awk "/^ *-a always,exit/ \
&&(/ -F auid!=unset/||/ -F auid==1/||/ -F auid!=4294967295/) \
&& -F auid>=${UID_MIN}/ \
&& -F perm=x/ \
&& -F path=/usr/bin/kmod/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S
init_module,finit_module,delete_module,create_module,query_module -F
auid>=1000 -F auid!=unset -k kernel_modules
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -
k kernel_modules
```

Running configuration

Run the following command to check loaded rules:

```

# auditctl -l | awk '/^ *-a *always,exit/ \
&& -F arch=b(32|64) / \
&&(/ -F auid!=unset/||/ -F auid==1/||/ -F auid!=4294967295/) \
&& -S/ \
&&(/init_module/ \
||/finit_module/ \
||/delete_module/ \
||/create_module/ \
||/query_module/) \
&&(/ key= *[^-~]* $/||/ -k *[^-~]* *$/)' 

# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
&& -F *auid>=${UID_MIN}/ \
&& -F *perm=x/ \
&& -F *path=/usr/bin/kmod/ \
&&(/ key= *[^-~]* $/||/ -k *[^-~]* *$/)" \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"

```

Verify the output includes:

```

-a always,exit -F arch=b64 -S
create_module,init_module,delete_module,query_module,finit_module -F
auid>=1000 -F auid==1 -F key=kernel_modules
-a always,exit -S all -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F
auid==1 -F key=kernel_modules

```

Symlink audit

Audit if the symlinks that `kmod` accepts is indeed pointing at it:

```

# S_LINKS=$(ls -l /usr/sbin/lsmod /usr/sbin/rmmod /usr/sbin/insmod
/usr/sbin/modinfo /usr/sbin/modprobe /usr/sbin/depmod | grep -v " ->
/bin/kmod" || true) \
&& if [[ "${S_LINKS}" != "" ]]; then printf "Issue with symlinks:
${S_LINKS}\n"; else printf "OK\n"; fi

```

Verify the output states `OK`. If there is a symlink pointing to a different location it should be investigated.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor kernel module modification.

64 Bit systems

Example:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# [ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S
init_module,finit_module,delete_module,create_module,query_module -F
auid>=${UID_MIN} -F auid!=unset -k kernel_modules
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k kernel_modules
" >> /etc/audit/rules.d/50-kernel_modules.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimised for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0004	M1047

4.2.3.20 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: This setting will require the system to be rebooted to update the active `auditd` configuration settings.

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:

```
# grep "\s*[^#]" /etc/audit/audit.rules | tail -1
```

Verify the output matches:

```
-e 2
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with `-e 2` at the end of the file.

Example:

```
# printf "
-e 2
" >> /etc/audit/rules.d/99-finalize.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	

4.2.3.21 Ensure the running and on disk configuration is the same (Manual)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The Audit system have both on disk and running configuration. It is possible for these configuration settings to differ.

Note: Due to the limitations of `augenrules` and `auditctl`, it is not absolutely guaranteed that loading the rule sets via `augenrules --load` will result in all rules being loaded or even that the user will be informed if there was a problem loading the rules.

Rationale:

Configuration differences between what is currently running and what is on disk could cause unexpected problems or may give a false impression of compliance requirements.

Audit:

Merged rule sets

Ensure that all rules in `/etc/audit/rules.d` have been merged into `/etc/audit/audit.rules`:

```
# augenrules --check  
/usr/sbin/augenrules: No change
```

Should there be any drift, run `augenrules --load` to merge and load all rules.

Remediation:

If the rules are not aligned across all three () areas, run the following command to merge and load all rules:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then echo "Reboot required to load rules"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (-e 2), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●

4.2.4 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.

DRAFT

4.2.4.1 Ensure audit log files are mode 0600 or less permissive (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Audit log files contain information about the system and system activity.

Rationale:

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

Audit:

Run the following command to verify audit log files have mode 0600 or less permissive:

```
# stat -Lc "%n %a" "$(dirname $( awk -F"=" '/^\\s*log_file\\s*=\\s*/ {print $2}' /etc/audit/auditd.conf | xargs ))/* | grep -v '[0,2,4,6]00'
```

Nothing should be returned

Remediation:

Run the following command to remove more permissive mode than 0600 from audit log files:

```
# find "$(dirname $( awk -F"=" '/^\\s*log_file\\s*=\\s*/ {print $2}' /etc/audit/auditd.conf | xargs ))" -type f \( ! -perm 600 -a ! -perm 0400 -a ! -perm 0200 -a ! -perm 0000 \| ) -exec chmod u-x,go-rwx {} +
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v7	<p>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.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.2.4.2 Ensure only authorized users own audit log files (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Audit log files contain information about the system and system activity.

Rationale:

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

Audit:

Run the following command to verify audit log files are owned by the `root` user:

```
# stat -Lc "%n %U" "$(dirname $(awk -F="#" '/^log_file\s*/ {print $2}' /etc/audit/auditd.conf | xargs))/* | grep -Pv -- '^H+\\h+root\\b'
```

Nothing should be returned

Remediation:

Run the following command to configure the audit log files to be owned by the `root` user:

```
# find $(dirname $(awk -F="#" '/^log_file\s*/ {print $2}' /etc/audit/auditd.conf | xargs)) -type f ! -user root -exec chown root {} +
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v7	<p>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.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.2.4.3 Ensure only authorized groups are assigned ownership of audit log files (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Audit log files contain information about the system and system activity.

Rationale:

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

Audit:

Run the following command to verify `log_group` parameter is set to either `adm` or `root` in `/etc/audit/auditd.conf`:

```
# grep -Piw -- '^h*log_group\h*=\h*(adm|root)\b' /etc/audit/auditd.conf
```

Verify the output is:

```
log_group = adm  
-OR-  
log_group = root
```

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" "$(dirname $(awk -F"=" '/^s*log_file\s*=\s*/ {print $2}' /etc/audit/auditd.conf | xargs))/* | grep -Pv '^h*\H+\h+(adm|root)\b'
```

Nothing should be returned

Remediation:

Run the following command to configure the audit log files to be owned by `adm` group:

```
# find $(dirname $(awk -F"=" '/^\\s*log_file\\s*=\\s*/ {print $2}') /etc/audit/auditd.conf | xargs) -type f \\( ! -group adm -a ! -group root \\) -exec chgrp adm {} +
```

Run the following command to configure the audit log files to be owned by the `adm` group:

```
# chgrp adm /var/log/audit/
```

Run the following command to set the `log_group` parameter in the audit configuration file to `log_group = adm`:

```
# sed -ri 's/^\\s*#?\\s*log_group\\s*=\\s*\\S+\\(\\s*#.*)?.*$/{log_group = adm\\1}' /etc/audit/auditd.conf
```

Run the following command to restart the audit daemon to reload the configuration file:

```
# systemctl restart auditd
```

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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.2.4.4 Ensure the audit log directory is 0750 or more restrictive (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The audit log directory contains audit log files.

Rationale:

Audit information includes all information including: audit records, audit settings and audit reports. This information is needed to successfully audit system activity. This information must be protected from unauthorized modification or deletion. If this information were to be compromised, forensic analysis and discovery of the true source of potentially malicious system activity is impossible to achieve.

Audit:

Run the following command to verify that the audit log directory has a mode of 0750 or less permissive:

```
# stat -Lc "%n %a" "$(dirname $( awk -F"=" '/^s*log_file\s*/ {print $2}' /etc/audit/auditd.conf))" | grep -Pv -- '^h*\H+\h+([0,5,7][0,5]0)'
```

Nothing should be returned

Remediation:

Run the following command to configure the audit log directory to have a mode of "0750" or less permissive:

```
# chmod g-w,o-rwx "$(dirname $( awk -F"=" '/^s*log_file\s*/ {print $2}' /etc/audit/auditd.conf))"
```

Default Value:

750

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v7	<p>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.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.2.4.5 Ensure audit configuration files are 640 or more restrictive (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Audit configuration files control auditd and what events are audited.

Rationale:

Access to the audit configuration files could allow unauthorized personnel to prevent the auditing of critical events.

Misconfigured audit configuration files may prevent the auditing of critical events or impact the system's performance by overwhelming the audit log. Misconfiguration of the audit configuration files may also make it more difficult to establish and investigate events relating to an incident.

Audit:

Run the following command to verify that the audit configuration files have mode 640 or more restrictive and are owned by the root user and root group:

```
# find /etc/audit/ -type f \(-name '*.conf' -o -name '*.rules'\) -exec stat -Lc "%n %a" {} + | grep -Pv -- '^\\h*\\H+\\h*([0,2,4,6][0,4]0)\\h*$'
```

Nothing should be returned

Remediation:

Run the following command to remove more permissive mode than 0640 from the audit configuration files:

```
# find /etc/audit/ -type f \(-name '*.conf' -o -name '*.rules'\) -exec chmod u-x,g-wx,o-rwx {} +
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v7	<p>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.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.2.4.6 Ensure audit configuration files are owned by root (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Audit configuration files control auditd and what events are audited.

Rationale:

Access to the audit configuration files could allow unauthorized personnel to prevent the auditing of critical events.

Misconfigured audit configuration files may prevent the auditing of critical events or impact the system's performance by overwhelming the audit log. Misconfiguration of the audit configuration files may also make it more difficult to establish and investigate events relating to an incident.

Audit:

Run the following command to verify that the audit configuration files have mode 640 or more restrictive and are owned by the root user and root group:

```
# find /etc/audit/ -type f \(-name '*.conf' -o -name '*.rules'\) ! -user root
```

Nothing should be returned

Remediation:

Run the following command to change ownership to root user:

```
# find /etc/audit/ -type f \(-name '*.conf' -o -name '*.rules'\) ! -user root -exec chown root {} +
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v7	<p>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.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.2.4.7 Ensure audit configuration files belong to group root (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Audit configuration files control auditd and what events are audited.

Rationale:

Access to the audit configuration files could allow unauthorized personnel to prevent the auditing of critical events.

Misconfigured audit configuration files may prevent the auditing of critical events or impact the system's performance by overwhelming the audit log. Misconfiguration of the audit configuration files may also make it more difficult to establish and investigate events relating to an incident.

Audit:

Run the following command to verify that the audit configuration files have mode 640 or more restrictive and are owned by the root user and root group:

```
# find /etc/audit/ -type f \(-name '*.conf' -o -name '*.rules'\) ! -group root
```

Nothing should be returned

Remediation:

Run the following command to change group to root:

```
# find /etc/audit/ -type f \(-name '*.conf' -o -name '*.rules'\) ! -group root -exec chgrp root {} +
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v7	<p>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.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.2.4.8 Ensure audit tools are 755 or more restrictive (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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.

Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Protecting audit tools is necessary to prevent unauthorized operation on audit information.

Audit:

Run the following command to verify the audit tools have mode 755 or more restrictive, are owned by the root user and group root:

```
# stat -c "%n %a" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/augenrules | grep -Pv -- '^h*\H+\h+([0-  
7][0,1,4,5][0,1,4,5])\h*$'
```

Nothing should be returned

Remediation:

Run the following command to remove more permissive mode from the audit tools:

```
# chmod go-w /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/augenrules
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v7	<p>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.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.2.4.9 Ensure audit tools are owned by root (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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.

Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Protecting audit tools is necessary to prevent unauthorized operation on audit information.

Audit:

Run the following command to verify the audit tools have mode 755 or more restrictive, are owned by the root user and group root:

```
# stat -c "%n %U" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/augenrules | grep -Pv -- '^h*\H+h+root\h*$'
```

Nothing should be returned

Remediation:

Run the following command to change the owner of the audit tools to the root user:

```
# chown root /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/augenrules
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v7	<p>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.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.2.4.10 Ensure audit tools belong to group root (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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.

Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Protecting audit tools is necessary to prevent unauthorized operation on audit information.

Audit:

Run the following command to verify the audit tools have mode 755 or more restrictive, are owned by the root user and group root:

```
# stat -c "%n %a %U %G" /sbin/auditctl /sbin/aureport /sbin/ausearch  
/sbin/autrace /sbin/auditd /sbin/augenrules | grep -Pv -- '^\\h*\\H+\\h+([0-  
7][0,1,4,5][0,1,4,5])\\h+root\\h+root\\h*$'
```

Nothing should be returned

Remediation:

Run the following command to remove more permissive mode from the audit tools:

```
# chmod go-w /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/augenrules
```

Run the following command to change owner and group of the audit tools to `root` user and group:

```
# chown root:root /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/augenrules
```

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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

4.2.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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.

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.

Attackers may 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.

Audit tools should 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 . Run the following command to verify that AIDE is configured to use cryptographic mechanisms to protect the integrity of audit tools:

```
# grep -P -- '(\/sbin\/(audit|au)\H*\b)' /etc/aide/aide.conf
```

Verify the output includes:

```
/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/augenrules p+i+n+u+g+s+b+acl+xattrs+sha512
```

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/augenrules p+i+n+u+g+s+b+acl+xattrs+sha512
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and 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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

5 Access, Authentication and Authorization

DRAFT

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
v7	6 <u>Maintenance, Monitoring and Analysis of Audit Logs</u> Maintenance, Monitoring and Analysis of Audit Logs			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	M1018

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002	M1018

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002	M1018

5.2 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.

Note:

- The recommendations in this section only apply if the SSH daemon is installed on the system, if remote access is **not** required the SSH daemon can be removed and this section skipped.
- Once all configuration changes have been made to `/etc/ssh/sshd_config`, the sshd configuration must be reloaded:

Command to re-load the SSH daemon configuration:

```
# systemctl reload sshd
```

Command to remove the SSH daemon:

```
# apt remove openssh-server
```

5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/ssh/sshd_config` file contains configuration specifications for `sshd`. The command below sets the owner and group of the file to `root`.

Rationale:

The `/etc/ssh/sshd_config` file needs to be protected from unauthorized changes by non-privileged users.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group or other`:

```
# stat /etc/ssh/sshd_config
```

Verify the output matches:

```
Access: (0600/-rw-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/ssh/sshd_config`:

```
# chown root:root /etc/ssh/sshd_config
# chmod og-rwx /etc/ssh/sshd_config
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098, T1098.004, T1543, T1543.002	TA0005	M1022

5.2.2 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 script to verify SSH private host key files are mode 0600 or more restrictive, owned be the root user, and owned be the group root or group designated to own openSSH private keys:

```
#!/usr/bin/env bash

{
    l_output=""
    l_skgn="ssh_keys" # Group designated to own openSSH keys
    l_skgid=$(awk -F: '$1 == "'$l_skgn'" {print $3}' /etc/group)
    awk '{print}' <<< "$(
        find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -
        exec stat -L -c "%n %#a %U %G %g" {} +)" | (
            while read -r l_file l_mode
            l_owner l_group l_gid; do
                [ -n "$l_skgid" ] && l_cga="$l_skgn" || l_cga="root"
                [ "$l_gid" = "$l_skgid" ] && l_pmask="0137" || l_pmask="0177"
                l_maxperm=$(( printf '%o' $(( 0777 & ~$l_pmask )) ))
                [ $(( $l_mode & $l_pmask )) -gt 0 ] && l_output="$l_output\n - File:
\"$l_file\" is mode \"$l_mode\" should be mode: \"$l_maxperm\" or more
restrictive"
                [ "$l_owner" != "root" ] && l_output="$l_output\n - File: \"$l_file\" is owned by: \"$l_owner\" should be owned by \"root\""
                if [ "$l_group" != "root" ] && [ "$l_gid" != "$l_skgid" ]; then
                    l_output="$l_output\n - File: \"$l_file\" is owned by group
\"$l_group\" should belong to group \"$l_cga\""
                fi
            done
            if [ -z "$l_output" ]; then
                echo -e "\n- Audit Result:\n    *** PASS ***\n"
            else
                echo -e "\n- Audit Result:\n    *** FAIL ***$l_output\n"
            fi
        )
    }
}
```

Remediation:

Run the following script to set mode, ownership, and group on the private SSH host key files:

```
#!/usr/bin/env bash

{
    l_skgn="ssh_keys" # Group designated to own openSSH keys
    l_skgid=$(awk -F: '$1 == "'"$l_skgn"'") {print $3}' /etc/group"
    awk '{print}' <<< "$({find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec stat -L -c "%n %#a %U %G %g" {} +)" | (while read -r l_file l_mode
    l_owner l_group l_gid; do
        [ -n "$l_skgid" ] && l_cga="$l_skgn" || l_cga="root"
        [ "$l_gid" = "$l_skgid" ] && l_pmask="0137" || l_pmask="0177"
        l_maxperm=$( printf '%o' $(( 0777 & ~$l_pmask )) )"
        if [ $(( $l_mode & $l_pmask )) -gt 0 ]; then
            echo -e " - File: \"$l_file\" is mode \"$l_mode\" changing to mode:
        \"$l_maxperm\""
            if [ -n "$l_skgid" ]; then
                chmod u-x,g-wx,o-rwx "$l_file"
            else
                chmod u-x,go-rwx "$l_file"
            fi
        fi
        if [ "$l_owner" != "root" ]; then
            echo -e " - File: \"$l_file\" is owned by: \"$l_owner\" changing
owner to \"root\""
            chown root "$l_file"
        fi
        if [ "$l_group" != "root" ] && [ "$l_gid" != "$l_skgid" ]; then
            echo -e " - File: \"$l_file\" is owned by group \"$l_group\" should
belong to group \"$l_cga\""
            chgrp "$l_cga" "$l_file"
        fi
    done
)
}
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v7	<p>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.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1552, T1552.004	TA0003, TA0006	M1022

5.2.3 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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0003, TA0006	M1022

5.2.4 Ensure SSH access is limited (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

- AllowUsers:
 - The `AllowUsers` variable gives the system administrator the option of allowing specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of `user@host`.
- AllowGroups:
 - The `AllowGroups` variable gives the system administrator the option of allowing specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.
- DenyUsers:
 - The `DenyUsers` variable gives the system administrator the option of denying specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of `user@host`.
- DenyGroups:
 - The `DenyGroups` variable gives the system administrator the option of denying specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

Rationale:

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Audit:

Run the following commands and verify the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -Pi '^h*(allow|deny) (users|groups) \h+\H+(\h+.*?)$'  
# grep -Pi '^h*(allow|deny) (users|groups) \h+\H+(\h+.*?)$' /etc/ssh/sshd_config
```

Verify that the output of both commands matches at least one of the following lines:

```
allowusers <userlist>  
allowgroups <grouplist>  
denyusers <userlist>  
denygroups <grouplist>
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set one or more of the parameter as follows:

```
AllowUsers <userlist>
```

OR

```
AllowGroups <grouplist>
```

OR

```
DenyUsers <userlist>
```

OR

```
DenyGroups <grouplist>
```

Default Value:

None

References:

1. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v7	<p>4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021, T1021.004	TA0008	M1018

5.2.5 Ensure SSH LogLevel is appropriate (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`INFO` level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

`VERBOSE` level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments.

Rationale:

SSH provides several logging levels with varying amounts of verbosity. `DEBUG` is specifically **not** recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

Audit:

Run the following command and verify that output matches `loglevel VERBOSE` or `loglevel INFO`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep loglevel  
loglevel VERBOSE or loglevel INFO
```

Run the following command and verify the output matches:

```
# grep -i 'loglevel' /etc/ssh/sshd_config | grep -Evi '(VERBOSE|INFO)'  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LogLevel VERBOSE
```

OR

```
LogLevel INFO
```

Default Value:

`LogLevel INFO`

References:

1. https://www.ssh.com/ssh/sshd_config/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	

5.2.6 Ensure SSH PAM is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `UsePAM` directive enables the Pluggable Authentication Module (PAM) interface. If set to `yes` this will enable PAM authentication using `ChallengeResponseAuthentication` and `PasswordAuthentication` directives 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

Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i usepam
```

Verify the output matches:

```
usepam yes
```

Run the following command:

```
# grep -Ei '^s*UsePAM\s+no' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
UsePAM yes
```

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021, T1021.004	TA0001	M1035

5.2.7 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. The default is `prohibit-password`.

Rationale:

Disallowing `root` logins over SSH requires system admins to authenticate using their own individual account, then escalating to `root`. This limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident.

Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permitrootlogin
```

Verify the output matches:

```
permitrootlogin no
```

Run the following command:

```
# grep -Ei '^s*PermitRootLogin\s+no' /etc/ssh/sshd_config
```

Verify the output matches:

```
PermitRootLogin no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitRootLogin no
```

Default Value:

`PermitRootLogin without-password`

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</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 Ensure the Use of Dedicated Administrative Accounts</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>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021	TA0008	M1042

5.2.8 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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep hostbasedauthentication
```

Verify the output matches:

```
hostbasedauthentication no
```

Run the following command:

```
# grep -Ei '^s*HostbasedAuthentication\s+yes' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
HostbasedAuthentication no
```

Default Value:

HostbasedAuthentication no

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>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.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0001	M1042

5.2.9 Ensure SSH PermitEmptyPasswords is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PermitEmptyPasswords` parameter specifies if the SSH server allows login to accounts with empty password strings.

Rationale:

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system.

Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permitemptypasswords
```

Verify the output matches:

```
permitemptypasswords no
```

Run the following command and verify the output:

```
# grep -Ei '^s*PermitEmptyPasswords\s+yes' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitEmptyPasswords no
```

Default Value:

`PermitEmptyPasswords no`

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>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.</p>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021	TA0008	M1042

5.2.10 Ensure SSH PermitUserEnvironment is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - 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 trojan'd programs)

Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permituserenvironment
```

Verify the output matches:

```
permituserenvironment no
```

Run the following command and verify the output:

```
# grep -Ei '^s*PermitUserEnvironment\s+yes' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitUserEnvironment no
```

Default Value:

PermitUserEnvironment no

References:

1. `SSHD_CONFIG(5)`

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021	TA0008	M1042

5.2.11 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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep ignorerhosts
```

Verify the output matches:

```
ignorerhosts yes
```

Run the following command:

```
# grep -Ei '^s*ignorerhosts\s+no\b' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
IgnoreRhosts yes
```

Default Value:

`IgnoreRhosts yes`

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0001	M1027

5.2.12 Ensure SSH X11 forwarding is disabled (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 2 - Server

Description:

The `X11Forwarding` parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.

Rationale:

Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i x11forwarding
```

Verify the output matches:

```
x11forwarding no
```

Run the following command:

```
# grep -Ei '^s*x11forwarding\s+yes' /etc/ssh/sshd_config
```

Nothing is returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
X11Forwarding no
```

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210, T1210.000	TA0008	M1042

5.2.13 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.
- The only "strong" ciphers currently FIPS 140-2 compliant are:
 - aes256-ctr
 - aes192-ctr
 - aes128-ctr
- Supported ciphers in openSSH 8.2:

```
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
```

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 Triple DES ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain clear text data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack.
- 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 plain text data from an arbitrary block of cipher text in an SSH session via unknown vectors.

Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep ciphers
```

Verify that output does not contain any of the following weak ciphers:

```
3des-cbc  
aes128-cbc  
aes192-cbc  
aes256-cbc
```

Remediation:

Edit the `/etc/ssh/sshd_config` file add/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](https://www.openssh.com/txt/cbc.adv),aes128-ctr,aes192-ctr,aes256-ctr,[aes128-gcm@openssh.com](https://www.openssh.com/txt/cbc.adv),[aes256-gcm@openssh.com](https://www.openssh.com/txt/cbc.adv)

References:

1. <https://nvd.nist.gov/vuln/detail/CVE-2016-2183>
2. <https://www.openssh.com/txt/cbc.adv>
3. <https://nvd.nist.gov/vuln/detail/CVE-2008-5161>
4. <https://www.openssh.com/txt/cbc.adv>
5. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1557	TA0006	M1041

5.2.14 Ensure only strong MAC algorithms are used (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This variable limits the types of MAC algorithms that SSH can use during communication.

Notes:

- Some organizations may have stricter requirements for approved MACs.
- Ensure that MACs used are in compliance with site policy.
- The only "strong" MACs currently FIPS 140-2 approved are:
 - hmac-sha2-256
 - hmac-sha2-512
- The Supported MACs are:

```
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
```

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i "MACs"
```

Verify that output does not contain any of the listed 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
```

Remediation:

Edit the `/etc/ssh/sshd_config` file and add/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)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1557, T1557.000	TA0006	M1041

5.2.15 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

Notes:

- *Kex algorithms have a higher preference the earlier they appear in the list*
- *Some organizations may have stricter requirements for approved Key exchange algorithms*
- *Ensure that Key exchange algorithms used are in compliance with site policy*
- *The only Key Exchange Algorithms currently FIPS 140-2 approved are:*
 - *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*
- *The Key Exchange algorithms supported by OpenSSH 8.2 are:*

```
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
```

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 that output does not contain any of the listed weak Key Exchange algorithms

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep kexalgorithms
```

Weak Key Exchange Algorithms:

```
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
```

Remediation:

Edit the /etc/ssh/sshd_config file add/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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1557, T1557.000	TA0006	M1041

5.2.16 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. In some 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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i allowtcpforwarding
```

Verify the output matches:

```
allowtcpforwarding no
```

Run the following command:

```
# grep -Ei '^s*AllowTcpForwarding\s+yes' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
AllowTcpForwarding no
```

Default Value:

AllowTcpForwarding yes

References:

1. <https://www.ssh.com/ssh/tunneling/example>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1048, T1048.002, T1572, T1572.000	TA0008	M1042

5.2.17 Ensure system-wide crypto policy is not over-ridden (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

System-wide Crypto policy can be over-ridden or opted out of for openSSH

Rationale:

Over-riding or opting out of the system-wide crypto policy could allow for the use of less secure Ciphers, MACs, KexAlgorithms and GSSAPIKexAlgorithm

Audit:

Run the following command:

```
# grep -i '^s*CRYPTO_POLICY=' /etc/sysconfig/sshd
```

No output should be returned

Remediation:

Run the following commands:

```
# sed -ri "s/^s*(CRYPTO_POLICY\s*=.*$/# \1/" /etc/sysconfig/sshd
# systemctl reload sshd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1557	TA0006	M1041

5.2.18 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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep banner
```

Verify the output matches:

```
banner /etc/issue.net
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Banner /etc/issue.net
```

CIS Controls:

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
	TA0001, TA0007	M1035

5.2.19 Ensure SSH MaxAuthTries is set to 4 or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxAuthTries` parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the `syslog` file detailing the login failure.

Rationale:

Setting the `MaxAuthTries` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Audit:

Run the following command and verify that output `MaxAuthTries` is 4 or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep maxauthtries  
maxauthtries 4
```

Run the following command and verify that the output:

```
# grep -Ei '^s*maxauthtries\s+([5-9]|1-9 [0-9]+)' /etc/ssh/sshd_config  
Nothing is returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxAuthTries 4
```

Default Value:

MaxAuthTries 6

References:

1. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.</p>		●	●
v7	<p>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>			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.003	TA0006	M1036

5.2.20 Ensure SSH MaxStartups is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxStartups` parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.

Rationale:

To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of `MaxStartups` to protect availability of sshd logins and prevent overwhelming the daemon.

Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i maxstartups
```

Verify that output `MaxStartups` is 10:30:60 or more restrictive:

```
maxstartups 10:30:60
```

Run the following command and verify the output:

```
# grep -Ei '^\\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]+) : ([0-9]+) : (6[1-9] | [7-9][0-9] | [1-9][0-9][0-9]+)))' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxStartups 10:30:60
```

Default Value:

MaxStartups 10:30:100

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.002	TA0040	

5.2.21 Ensure SSH MaxSessions is set to 10 or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxSessions` parameter specifies the maximum number of open sessions permitted from a given connection.

Rationale:

To protect a system from denial of service due to a large number of concurrent sessions, use the rate limiting function of `MaxSessions` to protect availability of `sshd` logins and prevent overwhelming the daemon.

Audit:

Run the following command and verify that output `MaxSessions` is 10 or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i maxsessions  
maxsessions 10
```

Run the following command and verify the output:

```
grep -Ei '^s*MaxSessions\s+(1[1-9]|2[0-9]|1[0-9]{2}|2[0-9]{2})' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxSessions 10
```

Default Value:

`MaxSessions 10`

References:

1. `SSHD_CONFIG(5)`

CIS Controls:

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.002	TA0040	

5.2.22 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
```

Verify the output matches:

```
logingracetime 60
```

Run the following command and verify the output:

```
# grep -Ei '^s*LoginGraceTime\s+(0|6[1-9]|7-9)[0-9]|1-9)[0-9][0-9]+|^1m' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LoginGraceTime 60
```

Default Value:

`LoginGraceTime 120`

References:

1. SSHD_CONFIG(5)

CIS Controls:

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.003, T1110.004, T1499, T1499.002	TA0006	M1036

5.2.23 Ensure SSH Idle Timeout Interval is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

NOTE: To clarify, the two settings described below is only meant for idle connections from a protocol perspective and not meant to check if the user is active or not. An idle user does not mean an idle connection. SSH does not and never had, intentionally, the capability to drop idle users. In SSH versions before 8.2p1 there was a bug that caused these values to behave in such a manner that they were abused to disconnect idle users. This bug has been resolved in 8.2p1 and thus it can no longer be abused to disconnect idle users.

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of SSH sessions. Taken directly from `man 5 sshd_config`:

- `ClientAliveInterval` Sets a timeout interval in seconds after which if no data has been received from the client, sshd(8) 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(8) 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. It is important to note that the use of client alive messages is very different from TCPKeepAlive. The client alive messages are sent through the encrypted channel and therefore will not be spoofable. The TCP keepalive option enabled by TCPKeepAlive is spoofable. The client alive mechanism is valuable when the client or server depend on knowing when a connection has become unresponsive. The default value is 3. If ClientAliveInterval is set to 15, and ClientAliveCountMax is left at the default, unresponsive SSH clients will be disconnected after approximately 45 seconds. Setting a zero ClientAliveCountMax disables connection termination.

Rationale:

In order to prevent resource exhaustion, appropriate values should be set for both `ClientAliveInterval` and `ClientAliveCountMax`. Specifically, looking at the source code, `ClientAliveCountMax` must be greater than zero in order to utilize the ability of SSH to drop idle connections. If connections are allowed to stay open indefinitely, this can potentially be used as a DDOS attack or simple resource exhaustion could occur over unreliable networks.

The example set here is a 45 second timeout. Consult your site policy for network timeouts and apply as appropriate.

Audit:

Run the following commands and verify `ClientAliveInterval` is greater than zero:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep clientaliveinterval
```

Example output:

```
clientaliveinterval 15
```

Run the following command and verify `ClientAliveCountMax` is greater than zero:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep clientalivecountmax
```

Example output:

```
clientalivecountmax 3
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameters according to site policy.

Example:

```
ClientAliveInterval 15  
ClientAliveCountMax 3
```

Default Value:

`ClientAliveInterval 0`

`ClientAliveCountMax 3`

References:

1. https://man.openbsd.org/sshd_config

Additional Information:

https://bugzilla.redhat.com/show_bug.cgi?id=1873547

https://github.com/openssh/openssh-portable/blob/V_8_9/serverloop.c#L137

CIS Controls:

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

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003	TA0001	M1026

5.3 Configure privilege escalation

There are various tools which allows a permitted user to execute a command as the superuser or another user, as specified by the security policy.

sudo

[sudo documentation](#)

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 plug-in architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plug-ins to work seamlessly with the `sudo` front end. The default security policy is `sudoers`, which is configured via the file `/etc/sudoers` and any entries in `/etc/sudoers.d`.

pkexec

[pkexec documentation](#)

`pkexec` allows an authorized user to execute *PROGRAM* as another user. If *username* is not specified, then the program will be executed as the administrative super user, `root`.

5.3.1 Ensure sudo is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

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 either `sudo` or `sudo-ldap` is installed.

Run the following command:

```
# dpkg -s sudo | grep "Status: "
# dpkg -s sudo-ldap | grep "Status: "
```

Verify the output matches the following for either one of the packages:

```
Status: install ok installed
```

Remediation:

First determine if LDAP functionality is required. If so, then install `sudo-ldap`, else install `sudo`.

Example:

```
# apt install sudo
```

References:

1. SUDO(8)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</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 Ensure the Use of Dedicated Administrative Accounts</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>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.003	TA0001	

5.3.2 Ensure sudo commands use pty (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`sudo` can be configured to run only from a pseudo terminal (pseudo-pty).

Rationale:

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

Impact:

WARNING: Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

Audit:

Verify that `sudo` can only run other commands from a pseudo terminal.

Run the following command:

```
# grep -rPi '^h*Defaults\h+([^\#\n\r]+,) ?use_pty(, \h*\h+\h*)*\h*(#.*)?$$' /etc/sudoers*
```

Verify the output matches:

```
/etc/sudoers:Defaults use_pty
```

Remediation:

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

```
Defaults use_pty
```

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</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>5.1 Establish Secure Configurations</p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.003	TA0003	

5.3.3 Ensure sudo log file exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo can use a custom log file

Rationale:

A sudo log file simplifies auditing of sudo commands

Impact:

WARNING: Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

Audit:

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

```
# grep -rPsi  
"^\h*Defaults\h+([^\#]+,\h*)?logfile\h*=\h*(\"|\')?\h+(\"|\')?(\,\h*\H+\h*)*\h*  
(#.*)?\$" /etc/sudoers*
```

Verify the output matches:

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

Remediation:

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

Example:

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

References:

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

Additional Information:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.</p>		●	●
v7	<p>6.3 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>		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0004	

5.3.4 Ensure users must provide password for privilege escalation (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The operating system must be configured so that users must provide a password for privilege escalation.

Rationale:

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

When operating systems provide the capability to escalate a functional capability, it is critical the user (re-)authenticate.

Impact:

This will prevent automated processes from being able to elevate privileges.

Audit:

Note: If passwords are not being used for authentication, this is not applicable.
Verify the operating system requires users to supply a password for privilege escalation.
Check the configuration of the /etc/sudoers and /etc/sudoers.d/* files with the following command:

```
# grep -r "^[^#].*NOPASSWD" /etc/sudoers*
```

If any line is found refer to the remediation procedure below.

Remediation:

Based on the outcome of the audit procedure, use visudo -f <PATH TO FILE> to edit the relevant sudoers file.

Remove any line with occurrences of NOPASSWD tags in the file.

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>	●	●	●

5.3.5 Ensure re-authentication for privilege escalation is not disabled globally (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The operating system must be configured so that users must re-authenticate for privilege escalation.

Rationale:

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

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

Audit:

Verify the operating system requires users to re-authenticate for privilege escalation. Check the configuration of the `/etc/sudoers` and `/etc/sudoers.d/*` files with the following command:

```
# grep -r "^[^#].*\!authenticate" /etc/sudoers*
```

If any line is found with a `!authenticate` tag, refer to the remediation procedure below.

Remediation:

Configure the operating system to require users to reauthenticate for privilege escalation.

Based on the outcome of the audit procedure, use `visudo -f <PATH TO FILE>` to edit the relevant sudoers file.

Remove any occurrences of `!authenticate` tags in the file(s).

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.	●	●	●

5.3.6 Ensure sudo authentication timeout is configured correctly (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`sudo` caches used credentials for a default of 15 minutes. This is for ease of use when there are multiple administrative tasks to perform. The timeout can be modified to suit local security policies.

This default is distribution specific. See audit section for further information.

Rationale:

Setting a timeout value reduces the window of opportunity for unauthorized privileged access to another user.

Audit:

Ensure that the caching timeout is no more than 15 minutes.

Example:

```
# grep -roP "timestamp_timeout=\K[0-9]*" /etc/sudoers*
```

If there is no `timestamp_timeout` configured in `/etc/sudoers*` then the default is 15 minutes. This default can be checked with:

```
# sudo -V | grep "Authentication timestamp timeout:"
```

NOTE: A value of `-1` means that the timeout is disabled. Depending on the configuration of the `timestamp_type`, this could mean for all terminals / processes of that user and not just that one single terminal session.

Remediation:

If the currently configured timeout is larger than 15 minutes, edit the file listed in the audit section with `visudo -f <PATH TO FILE>` and modify the entry `timestamp_timeout=` to 15 minutes or less as per your site policy. The value is in minutes. This particular entry may appear on it's own, or on the same line as `env_reset`. See the following two examples:

```
Defaults    env_reset, timestamp_timeout=15
Defaults    timestamp_timeout=15
Defaults    env_reset
```

References:

1. <https://www.sudo.ws/man/1.9.0/sudoers.man.html>

CIS Controls:

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

5.3.7 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 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:

```
# grep -Pi '^auth[ ]+required[ ]+pam_wheel\.so[ ]+group=[^#\'n\']+[ ]+use_uid\b|group=\H+\b)' /etc/pam.d/su
```

Verify the output matches:

```
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
```

Verify the output does not contain any users in the relevant group:

```
<group_name>:x:<GID>:
```

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:

```
auth required pam_wheel.so use_uid group=sugroup
```

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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.000	TA0005	M1026

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.

Note: The usage of `pam-auth-update`:

- As of this writing, the management of PAM via `pam-auth-update` does not offer all the required functionality implemented by the benchmark. As such, the usage of `pam-auth-update` is not recommended at present.

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 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

Rationale:

Strong passwords protect systems from being hacked through brute force methods.

Audit:

Verify password creation requirements conform to organization policy.

Password length

Run the following command:

```
# grep '^s*minlen\s*' /etc/security/pwquality.conf
```

Verify the output matches:

```
minlen = 14
```

Password complexity

Option 1

Run the following command:

```
# grep '^s*minclass\s*' /etc/security/pwquality.conf
```

Verify the output matches:

```
minclass = 4
```

Option 2

Run the following command:

```
# grep -E '^s*[duol]credit\s*' /etc/security/pwquality.conf
```

Verify the output matches:

```
dcredit = -1  
ucredit = -1  
lcredit = -1  
ocredit = -1
```

Remediation:

The following setting is a recommend example policy. Alter these values to conform to your own organization's password policies.

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:

Option 1

```
minclass = 4
```

Option 2

```
dcredit = -1  
ucredit = -1  
ocredit = -1  
lcredit = -1
```

Additional Information:

Additional module options may be set, recommendation requirements only cover including `try_first_pass` and `minlen` set to 14 or more.

NOTE: As of this writing it is not possible to customize the maximum number of retries for the creation of a password within recommended methods. The command `pam-auth-update` is used to manage certain PAM configurations via profiles, such as `/etc/pam.d/common-password`. Making a manual change to this file will cause `pam-auth-update` to overwrite it on the next run and is thus against recommendations.

Alternatively, `pam_pwquality` (via `/etc/security/pwquality.conf`) fully supports the configuration of the maximum number of retries for a password change with the configuration entry `retry = xxx`. The issue is that the template `/usr/share/pam-configs/pwquality` contains `retry=3` which will override any retry setting in `/etc/security/pwquality.conf` as PAM entries takes precedence. This template file should not be modified as any package update will overwrite the change. Thus it is not possible, in any recommended way, to modify password retries.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.001, T1110.002, T1110.003	TA0006	M1027

5.4.2 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 common 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.

All configuration of `faillock` is located in `/etc/security/faillock.conf` and well commented.

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.

Impact:

It is critical to test and validate any PAM changes before deploying. Any misconfiguration could cause the system to be inaccessible.

Audit:

Verify password lockouts are configured. These settings are commonly configured with the `pam_faillock.so` module found in `/etc/pam.d/common-auth` and `/etc/pam.d/common-account`.

Common auth

Run the following command:

```
# grep "pam_faillock.so" /etc/pam.d/common-auth
```

Verify the output matches:

```
auth required pam_faillock.so  
auth [default=die] pam_faillock.so authfail
```

Common account

Run the following command:

```
# grep "pam_faillock.so" /etc/pam.d/common-account
```

Verify the output matches:

```
account required pam_faillock.so
```

Fail lock configuration

Run the following command:

```
awk '/^ *deny *=/\\n|/^\*fail_interval *=/\\n|/^\*unlock_time *=/' /etc/security/faillock.conf
```

Verify the output matches your site policy:

```
deny = 4  
fail_interval = 900  
unlock_time = 60
```

Remediation:

NOTE: Pay special attention to the configuration. Incorrect configuration can cause system lock outs. This is example configuration. Your configuration may differ based on previous changes to the files.

Common auth

Edit `/etc/pam.d/common-auth` and ensure that `faillock` is configured.

NOTE: It is critical to understand each line and the relevant arguments for successful implementation. The order of these entries is very specific.

```
auth    required          pam_faillock.so
auth    [success=2 default=ignore]  pam_unix.so nullok
auth    [default=die]  pam_faillock.so      authfail
auth    requisite        pam_deny.so
auth    required          pam_permit.so
```

Common account

Edit `/etc/pam.d/common-account` and ensure that the following stanza is at the end of the file.

```
account  required  pam_faillock.so
```

Fail lock configuration

Edit `/etc/security/faillock.conf` and configure it per your site policy.

Additional Information:

- If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_faillock.so` module, the user can be unlocked by issuing the command `/usr/sbin/faillock --user 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.003	TA0006	M1027

5.4.3 Ensure password reuse is limited (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/security/opasswd` file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

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 command:

```
# grep -P
'^\h*password\h+([^\#\n\r]+)\h+?pam_unix\.so\h+([^\#\n\r]+)\h+?remember=([5-
9]|1[1-9][0-9]+)\b' /etc/pam.d/common-password
```

Verify the output matches:

```
password      [success=1 default=ignore]      pam_unix.so obscure
use_authtok try_first_pass yesCRYPT remember=5
```

Ensure the `remember` option is 5 or more per your site policy.

Remediation:

NOTE: Pay special attention to the configuration. Incorrect configuration can cause system lock outs. This is example configuration. Your configuration may differ based on previous changes to the files.

Edit the `/etc/pam.d/common-password` file to include the `remember` option and conform to site policy as shown:

```
password      [success=1 default=ignore]      pam_unix.so obscure
use_authtok try_first_pass yesCRYPT remember=5
```

Additional Information:

Changes only apply to accounts configured on the local system.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.004		

5.4.4 Ensure password hashing algorithm is up to date with the latest standards (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The commands below change password encryption to `yescrypt`. All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.

Rationale:

The `yescrypt` algorithm provides much stronger hashing than previous available algorithms, 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:

PAM

No hashing algorithm should be configured in `/etc/pam.d/common-password`.

Run the following command:

```
# grep -v ^# /etc/pam.d/common-password | grep -E  
"(yescrypt|md5|bigcrypt|sha256|sha512|blowfish)"
```

Verify that there is no output.

If there is a business requirement to configure the hashing algorithm in PAM, ensure that the same algorithm is configured in `/etc/login.defs`.

Login definitions

Run the following command:

```
# grep "^\s*ENCRYPT_METHOD\s*yescrypt\s*\$" /etc/login.defs
```

Verify the output matches:

```
ENCRYPT_METHOD yescrypt
```

Remediation:

NOTE: Pay special attention to the configuration. Incorrect configuration can cause system lock outs. This is example configuration. Your configuration may differ based on previous changes to the files.

PAM

Edit the `/etc/pam.d/common-password` file and ensure that no hashing algorithm option for `pam_unix.so` is set:

```
password      [success=1 default=ignore]      pam_unix.so obscure use_authtok  
try_first_pass remember=5
```

Login definitions

Edit `/etc/login.defs` and ensure that `ENCRYPT_METHOD` is set to `yescrypt`.

Additional Information:

Additional module options may be set, recommendation only covers those listed here.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1110, T1110.002	TA0006	M1041

5.4.5 Ensure all current passwords uses the configured hashing algorithm (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Currently used passwords with out of date hashing algorithms may pose a security risk to the system.

Rationale:

In use passwords should always match the configured hashing algorithm for the system.

Impact:

If the administrator forces a password change, this could cause a large spike in CPU usage if a large number of users change their password during the same time.

Audit:

To get a list of users that is not using the currently configured hashing algorithm, run the following command:

```
# declare -A HASH_MAP=( ["y"]="yescrypt" ["1"]="md5" ["2"]="blowfish"
["5"]="SHA256" ["6"]="SHA512" ["g"]="gost-yescrypt" )
# CONFIGURED_HASH=$(sed -n "s/^$CURRENT_HASH\s*\(\.*\)\s*/\1/p"
/etc/login.defs)

# for MY_USER in $(sed -n "s/^(\.*):\$\.*/\1/p" /etc/shadow)
do
    CURRENT_HASH=$(sed -n "s/\${MY_USER}:\$\(\.\)\.*/\1/p" /etc/shadow)
    if [[ "\${HASH_MAP["\$CURRENT_HASH"]}" != "\${CONFIGURED_HASH}" ]]; then
        echo "The password for '\${MY_USER}' is using
'\${HASH_MAP["\$CURRENT_HASH"]}' instead of the configured
'\${CONFIGURED_HASH}'."
    fi
done
```

Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

Remediation:

If the administrator wish to force an immediate change on all users as per the output of the audit, execute:

```
# UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
# awk -F: -v UID_MIN="$UID_MIN" '$3 >= UID_MIN && $1 != "nfsnobody" { print $1 }' /etc/passwd | xargs -n 1 chage -d 0
```

NOTE: This could cause significant temporary CPU load on the system if a large number of users reset their passwords at the same time.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1110, T1110.002	TA0006	M1041

5.5 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

DRAFT

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.

DRAFT

5.5.1.1 Ensure minimum days between password changes is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PASS_MIN_DAYS` parameter in `/etc/login.defs` allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that `PASS_MIN_DAYS` parameter be set to 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`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>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.</p>		●	●
v6	<p>16 Account Monitoring and Control Account Monitoring and Control</p>			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.004	TA0006	M1027

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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.001, T1110.002, T1110.003, T1110.004		

5.5.1.3 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
	TA0006	M1027

5.5.1.4 Ensure inactive password lock is 30 days or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Audit:

Run the following command and verify INACTIVE conforms to site policy (no more than 30 days):

```
# useradd -D | grep INACTIVE
INACTIVE=30
```

Verify all users with a password have Password inactive no more than 30 days after password expires:

Run the following command and Review list of users and INACTIVE to verify that all users' INACTIVE conforms to site policy (no more than 30 days):

```
# 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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.002, T1078.003	TA0001	M1027

5.5.1.5 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.001, T1110.002, T1110.003, T1110.004		

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
v7	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0005	M1026

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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.000	TA0005	M1026

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\st+\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][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*
```

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][0-6]\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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1565, T1565.001	TA0007	

5.5.5 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+;\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+;\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
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003	TA0005	M1026

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.

DRAFT

6.1 System File Permissions

This section provides guidance on securing aspects of system files and directories.

DRAFT

6.1.1 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
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

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 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
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.3 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
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

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 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	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.5 Ensure permissions on /etc/shadow are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/shadow` file is used to store 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
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

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 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 from `/etc/shadow-`:

```
# chmod u-x,g-wx,o-rwx /etc/shadow-
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.7 Ensure permissions on /etc/gshadow are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/gshadow` file is used to store 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
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

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 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
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.9 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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

6.1.10 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
v7	<p>13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization</p> <p>Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0007	

6.1.11 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
v7	<p>13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization</p> <p>Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0007	

6.1.12 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
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0004	M1028

6.1.13 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
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0004	M1028

6.2 Local User and Group Settings

This section provides guidance on securing aspects of the local 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.

DRAFT

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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008	TA0003	M1027

6.2.2 Ensure /etc/shadow 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
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0003	M1027

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
v7	<p>16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.</p>		●	●
v7	<p>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.</p>		●	●
v7	<p>16.8 Disable Any Unassociated Accounts Disable any account that cannot be associated with a business process or business owner.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0003	M1027

6.2.4 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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008	TA0005	M1022

6.2.5 Ensure no duplicate UIDs exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0005	M1027

6.2.6 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
v7	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0005	M1027

6.2.7 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
v7	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0004	M1027

6.2.8 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
v7	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0004	M1027

6.2.9 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 a 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
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0006	M1022

6.2.10 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
v7	4.6 Use of Dedicated Machines For All Administrative Tasks 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.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.000	TA0001	M1026

6.2.11 Ensure local interactive user home directories exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Users can be defined in `/etc/passwd` without a home directory or with a home directory that does not actually exist.

Rationale:

If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

Audit:

Run the following script to verify all local interactive user home directories exist:

```
#!/usr/bin/env bash

{
    output=""
    valid_shells="^$( sed -rn '/^//{s,/,\\\\\\/,g;p}' /etc/shells | paste -s -d '|' - )$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd | (while read -r user home; do
    [ ! -d "$home" ] && output="$output\n - User \"$user\" home directory
\"$home\" doesn't exist"
    done
    if [ -z "$output" ]; then
        echo -e "\n-PASSED: - All local interactive users have a home
directory\n"
    else
        echo -e "\n- FAILED:\n$output\n"
    fi
)
}
```

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:

```
#!/usr/bin/env bash

{
    valid_shells="^(\$( sed -rn '/^//{s,/,\\\\\\/,g;p}' /etc/shells | paste -s -
d '|')\$"
    awk -v pat="$valid_shells" -F: '\$NF ~ pat { print $1 " " $(NF-1) }'
/etc/passwd | while read -r user home; do
    if [ ! -d "$home" ]; then
        echo -e "\n- User \"$user\" home directory \"$home\" doesn't
exist\n- creating home directory \"$home\"\n"
        mkdir "$home"
        chmod g-w,o-wrx "$home"
        chown "$user" "$home"
    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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
	TA0005	M1022

6.2.12 Ensure local interactive 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 to verify local interactive users own their home directories:

```
#!/usr/bin/env bash

{
    output=""
    valid_shells="^($( sed -rn '/^\/\//{s,/,\\\\\\/,g;p}' /etc/shells | paste -s -d '|' - ))$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }' /etc/passwd | (while read -r user home; do
        owner=$(stat -L -c "%U" "$home")
        [ "$owner" != "$user" ] && output="$output\n - User \"$user\" home
directory \"$home\" is owned by user \"$owner\""
        done
        if [ -z "$output" ]; then
            echo -e "\n-PASSED: - All local interactive users have a home
directory\n"
        else
            echo -e "\n- FAILED:\n$output\n"
        fi
    )
}
```

Remediation:

Change the ownership of any home directories that are not owned by the defined user to the correct user.

The following script will update local interactive user home directories to be own by the user:

```
#!/usr/bin/env bash

{
    output=""
    valid_shells="^$( sed -rn '/^//{s,,\\\,\g;p}' /etc/shells | paste -s -d '|' - )$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }' /etc/passwd | while read -r user home; do
        owner=$(stat -L -c "%U" "$home")
        if [ "$owner" != "$user" ]; then
            echo -e "\n- User \"$user\" home directory \"$home\" is owned by user \"$owner\"\n- changing ownership to \"$user\"\n"
            chown "$user" "$home"
        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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

6.2.13 Ensure local interactive user home directories are mode 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 verify interactive user home directories are mode 750 or more restrictive:

```
#!/usr/bin/env bash

{
    output=""
    perm_mask='0027'
    maxperm=$( printf '%o' $(( 0777 & ~$perm_mask)) )
    valid_shells=$( $( sed -rn '/^\\//{s,/,\\\\\\\\/,g;p}' /etc/shells | paste -s -d '|' - ) )$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd | (while read -r user home; do
    mode=$( stat -L -c '%#a' "$home" )
    [ $(( $mode & $perm_mask )) -gt 0 ] && output="$output\n- User $user
home directory: \"$home\" is too permissive: \"$mode\" (should be:
\"$maxperm\" or more restrictive)"
    done
    if [ -n "$output" ]; then
        echo -e "\n- Failed:$output"
    else
        echo -e "\n- Passed:\n- All user home directories are mode:
\"$maxperm\" or more restrictive"
    fi
)
}
```

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 interactive user home directories:

```
#!/usr/bin/env bash

{
    perm_mask='0027'
    maxperm=$( printf '%o' $(( 0777 & ~$perm_mask )) )
    valid_shells="^($( sed -rn '/^//{s,/,\\\/,g;p}' /etc/shells | paste -s -d '|' - )$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd | (while read -r user home; do
    mode=$( stat -L -c '%#a' "$home" )
    if [ $(( $mode & $perm_mask )) -gt 0 ]; then
        echo -e "- modifying User $user home directory: \"$home\"\n- removing excessive permissions from current mode of \"$mode\""
        chmod g-w,o-rwx "$home"
    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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

6.2.14 Ensure no local interactive user has .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.

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.

```
#!/usr/bin/env bash

{
    output="" output2=""
    perm_mask='0177'
    maxperm=$( printf '%o' $(( 0777 & ~$perm_mask)) )
    valid_shells="^($( sed -rn '/^\\//{s,,\\\\\\/,g;p}' /etc/shells | paste -s -d '|') - )$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd | (while read -r user home; do
    if [ -f "$home/.netrc" ]; then
        mode=$( stat -L -c '%#a' "$home/.netrc" )
        if [ $(($mode & $perm_mask)) -gt 0 ]; then
            output="$output\n - User \"$user\" file: \"$home/.netrc\" is too
permissive: \"$mode\" (should be: \"$maxperm\" or more restrictive)"
        else
            output2="$output2\n - User \"$user\" file: \"$home/.netrc\""
        exists and has file mode: \"$mode\" (should be: \"$maxperm\" or more
restrictive)"
        fi
    fi
done
if [ -z "$output" ]; then
    if [ -z "$output2" ]; then
        echo -e "\n-PASSED: - No local interactive users have \".netrc\""
files in their home directory\n"
    else
        echo -e "\n- WARNING:$output2\n"
    fi
else
    echo -e "\n- FAILED:$output\n"
    [ -n "$output2" ] && echo -e "\n- WARNING:$output2\n"
fi
)
}
```

Verify:

- Any lines under 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 under 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

```
#!/usr/bin/env bash

{
    perm_mask='0177'
    valid_shells="^($ sed -rn '/^//{s,/,\n/g;p}' /etc/shells | paste -s -
d '||-')$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd | while read -r user home; do
    if [ -f "$home/.netrc" ]; then
        echo -e "\n- User \"$user\" file: \"$home/.netrc\" exists\n-
removing file: \"$home/.netrc\"\n"
        rm -f "$home/.netrc"
    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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1152, T1552.001	TA0006	M1027

6.2.15 Ensure no local interactive user has .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:

```
#!/usr/bin/env bash

{
    output=""
    fname=".forward"
    valid_shells="^$( sed -rn '/^\\//{s,/,\\\\\\,g;p}' /etc/shells | paste -s -d '|' - )$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd | (while read -r user home; do
    [ -f "$home/$fname" ] && output="$output\n - User \"$user\" file:
\"$home/$fname\" exists"
    done
    if [ -z "$output" ]; then
        echo -e "\n-PASSED: - No local interactive users have \"$fname\""
files in their home directory\n"
    else
        echo -e "\n- FAILED:\n$output\n"
    fi
)
}
```

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

```
#!/usr/bin/env bash

{
    output=""
    fname=".forward"
    valid_shells="^(\$( sed -rn '/^\\//{s,/,\\\\\\/,g;p}' /etc/shells | paste -s -d '|' - ))$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd | (while read -r user home; do
    if [ -f "$home/$fname" ]; then
        echo -e "$output\n- User \"$user\" file: \"$home/$fname\" exists\n- removing file: \"$home/$fname\"\n"
        rm -r "$home/$fname"
    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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1114, T1114.003	TA0010	M1031

6.2.16 Ensure no local interactive user has .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 to verify no local interactive user has .rhosts files:

```
#!/usr/bin/env bash

{
    output=""
    fname=".rhosts"
    valid_shells="^$( sed -rn '/^\\/{s,,\\\\\\,g;p}' /etc/shells | paste -s -d '|' - )$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd | (while read -r user home; do
    [ -f "$home/$fname" ] && output="$output\n - User \"$user\" file:
\"$home/$fname\" exists"
    done
    if [ -z "$output" ]; then
        echo -e "\n-PASSED: - No local interactive users have \"$fname\" files in their home directory\n"
    else
        echo -e "\n- FAILED:\n$output\n"
    fi
)
}
```

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

```
#!/usr/bin/env bash

{
    perm_mask='0177'
    valid_shells="^($ sed -rn '/^//{s,/,\n/g;p}' /etc/shells | paste -s -
d '||-')$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd | while read -r user home; do
    if [ -f "$home/.rhosts" ]; then
        echo -e "\n- User \"$user\" file: \"$home/.rhosts\" exists\n-
removing file: \"$home/.rhosts\"\n"
        rm -f "$home/.rhosts"
    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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1049, T1049.000	TA0007	

6.2.17 Ensure local interactive user 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 to verify local interactive user dot files are not group or world writable:

```
#!/usr/bin/env bash

{
    output=""
    perm_mask='0022'
    maxperm=$( printf '%o' $(( 0777 & ~$perm_mask)) )
    valid_shells=$( $( sed -rn '/^\\//{s,/,\\\\\\\\/,g;p}' /etc/shells | paste -s -d '|' - ) )$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd | (while read -r user home; do
    for dfile in $(find "$home" -type f -name '.*'); do
        mode=$( stat -L -c '%#a' "$dfile" )
        [ $(( $mode & $perm_mask )) -gt 0 ] && output="$output\n- User $user
file: \"$dfile\" is too permissive: \"$mode\" (should be: \"$maxperm\" or
more restrictive)"
        done
    done
    if [ -n "$output" ]; then
        echo -e "\n- Failed:$output"
    else
        echo -e "\n- Passed:\n- All user home dot files are mode: \"$maxperm\""
    or more restrictive"
        fi
    )
}
```

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.

```
#!/usr/bin/env bash

{
    perm_mask='0022'
    valid_shells="^$( sed -rn '/^\\//{s,/,\\\\\\,g;p}' /etc/shells | paste -s -
d '|' - )$"
    awk -v pat="$valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd | while read -r user home; do
    find "$home" -type f -name '.*' | while read -r dfile; do
        mode=$( stat -L -c '%#a' "$dfile" )
        if [ $(( $mode & $perm_mask )) -gt 0 ]; then
            echo -e "\n- Modifying User \"$user\" file: \"$dfile\"\n-
removing group and other write permissions"
            chmod go-w "$dfile"
        fi
    done
done
}
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v7	<p>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.</p>	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.001, T1222.002, T1552, T1552.003, T1552.004	TA0005	M1022

Appendix: Summary Table

CIS Benchmark Recommendation		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 squashfs filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure mounting of udf filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Configure /tmp		
1.1.2.1	Ensure /tmp is a separate partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2	Ensure nodev option set on /tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3	Ensure noexec option set on /tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4	Ensure nosuid option set on /tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Configure /var		
1.1.3.1	Ensure separate partition exists for /var (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3.2	Ensure nodev option set on /var partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3.3	Ensure noexec option set on /var partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3.4	Ensure nosuid option set on /var partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Configure /var/tmp		
1.1.4.1	Ensure separate partition exists for /var/tmp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.1.4.2	Ensure noexec option set on /var/tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4.3	Ensure nosuid option set on /var/tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4.4	Ensure nodev option set on /var/tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Configure /var/log		
1.1.5.1	Ensure separate partition exists for /var/log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5.2	Ensure nodev option set on /var/log partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5.3	Ensure noexec option set on /var/log partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5.4	Ensure nosuid option set on /var/log partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	Configure /var/log/audit		
1.1.6.1	Ensure separate partition exists for /var/log/audit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6.2	Ensure noexec option set on /var/log/audit partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6.3	Ensure nodev option set on /var/log/audit partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6.4	Ensure nosuid option set on /var/log/audit partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Configure /home		
1.1.7.1	Ensure separate partition exists for /home (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7.2	Ensure nodev option set on /home partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.1.7.3	Ensure nosuid option set on /home partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7.4	Ensure usrquota option set on /home partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7.5	Ensure grpquota option set on /home partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Configure /dev/shm		
1.1.8.1	Ensure nodev option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8.2	Ensure noexec option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8.3	Ensure nosuid option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Disable Automounting (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Disable USB Storage (Automated)	<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"/>
1.3	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"/>
1.4	Secure Boot Settings		
1.4.1	Ensure bootloader password is set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.4.2	Ensure permissions on bootloader config are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Ensure authentication required for single user mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Additional Process Hardening		
1.5.1	Ensure XD/NX support is enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure address space layout randomization (ASLR) is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Ensure prelink is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Ensure core dumps are restricted (Automated)	<input type="checkbox"/>	<input 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 type="checkbox"/>
1.6.1.2	Ensure AppArmor is enabled in the bootloader configuration (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.1.3	Ensure all AppArmor Profiles are in enforce or complain mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.1.4	Ensure all AppArmor Profiles are enforcing (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Command Line Warning Banners		
1.7.1	Ensure message of the day is configured properly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.2	Ensure local login warning banner is configured properly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.3	Ensure remote login warning banner is configured properly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.7.4	Ensure permissions on /etc/motd are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.5	Ensure permissions on /etc/issue are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.6	Ensure permissions on /etc/issue.net are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8	GNOME Display Manager		
1.8.1	Ensure GNOME Display Manager is removed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.2	Ensure GDM login banner is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.3	Ensure disable-user-list option is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.4	Ensure GDM screen locks when the user is idle (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.5	Ensure GDM screen locks can not be overridden (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.6	Ensure automatic mounting of removable media is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8.7	Ensure XDCMP is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure updates, patches, and additional security software are installed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2	Services		
2.1	Configure Time Synchronization		
2.1.1	Ensure time synchronization is in use		
2.1.1.1	Ensure a single time synchronization daemon is in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Configure chrony		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.2.1	Ensure chrony is configured with authorized timeserver (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2.2	Ensure chrony is running as user _chrony (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2.3	Ensure chrony is enabled and running (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Configure systemd-timesyncd		
2.1.3.1	Ensure systemd-timesyncd configured with authorized timeserver (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3.2	Ensure systemd-timesyncd is enabled and running (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Configure ntp		
2.1.4.1	Ensure ntp access control is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4.2	Ensure ntp is configured with authorized timeserver (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4.3	Ensure ntp is running as user ntp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4.4	Ensure ntp is enabled and running (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Special Purpose Services		
2.2.1	Ensure X Window System is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure Avahi Server is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure CUPS is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure DHCP Server is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure LDAP server is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure NFS is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Ensure DNS Server is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.8	Ensure FTP Server is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	Ensure HTTP server is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	Ensure IMAP and POP3 server are not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure Samba is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.12	Ensure HTTP Proxy Server is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure SNMP Server is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	Ensure NIS Server is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	Ensure mail transfer agent is configured for local-only mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	Ensure rsync service is either not installed or masked (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Service Clients		
2.3.1	Ensure NIS Client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure rsh client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure talk client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure telnet client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure LDAP client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6	Ensure RPC is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure nonessential services are removed or masked (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3	Network Configuration		
3.1	Disable unused network protocols and devices		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.1	Ensure system is checked to determine if IPv6 is enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure wireless interfaces are disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Network Parameters (Host Only)		
3.2.1	Ensure packet redirect sending is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure IP forwarding is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Network Parameters (Host and Router)		
3.3.1	Ensure source routed packets are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure ICMP redirects are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure secure ICMP redirects are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure suspicious packets are logged (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure broadcast ICMP requests are ignored (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure bogus ICMP responses are ignored (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.7	Ensure Reverse Path Filtering is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.8	Ensure TCP SYN Cookies is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure IPv6 router advertisements are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Uncommon Network Protocols		
3.4.1	Ensure DCCP is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2	Ensure SCTP is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3	Ensure RDS is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.4.4	Ensure TIPC is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Firewall Configuration		
3.5.1	Configure UncomplicatedFirewall		
3.5.1.1	Ensure ufw is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.1.2	Ensure iptables-persistent is not installed with ufw (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.1.3	Ensure ufw service is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.1.4	Ensure ufw loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.1.5	Ensure ufw outbound connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.1.6	Ensure ufw firewall rules exist for all open ports (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.1.7	Ensure ufw default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2	Configure nftables		
3.5.2.1	Ensure nftables is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2.2	Ensure ufw is uninstalled or disabled with nftables (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2.3	Ensure iptables are flushed with nftables (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2.4	Ensure a nftables table exists (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2.5	Ensure nftables base chains exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2.6	Ensure nftables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2.7	Ensure nftables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.5.2.8	Ensure nftables default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2.9	Ensure nftables service is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2.10	Ensure nftables rules are permanent (Automated)	<input type="checkbox"/>	<input 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 type="checkbox"/>
3.5.3.1.2	Ensure nftables is not installed with iptables (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3.1.3	Ensure ufw is uninstalled or disabled with iptables (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3.2	Configure IPv4 iptables		
3.5.3.2.1	Ensure iptables default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3.2.2	Ensure iptables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3.2.3	Ensure iptables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3.2.4	Ensure iptables firewall rules exist for all open ports (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3.3	Configure IPv6 ip6tables		
3.5.3.3.1	Ensure ip6tables default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3.3.2	Ensure ip6tables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3.3.3	Ensure ip6tables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3.3.4	Ensure ip6tables firewall rules exist for all open ports (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4	Logging and Auditing		
4.1	Configure Logging		
4.1.1	Configure journald		
4.1.1.1	Ensure journald is configured to send logs to a remote log host		
4.1.1.1.1	Ensure systemd-journal-remote is installed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1.2	Ensure systemd-journal-remote is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1.3	Ensure systemd-journal-remote is enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1.4	Ensure journald is not configured to receive logs from a remote client (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Ensure journald service is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.3	Ensure journald is configured to compress large log files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	Ensure journald is configured to write logfiles to persistent disk (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.5	Ensure journald is not configured to send logs to rsyslog (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.6	Ensure journald log rotation is configured per site policy (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.7	Ensure journald default file permissions configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Configure rsyslog		
4.1.2.1	Ensure rsyslog is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.2	Ensure rsyslog service is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.3	Ensure journald is configured to send logs to rsyslog (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1.2.4	Ensure rsyslog default file permissions are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.5	Ensure logging is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.6	Ensure rsyslog is configured to send logs to a remote log host (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.7	Ensure rsyslog is not configured to receive logs from a remote client (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure all logfiles have appropriate permissions and ownership (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Configure System Accounting (auditd)		
4.2.1	Ensure auditing is enabled		
4.2.1.1	Ensure auditd is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.2	Ensure auditd service is enabled and active (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.3	Ensure auditing for processes that start prior to auditd is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1.4	Ensure audit_backlog_limit is sufficient (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	Configure Data Retention		
4.2.2.1	Ensure audit log storage size is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.2	Ensure audit logs are not automatically deleted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2.3	Ensure system is disabled when audit logs are full (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Configure auditd rules		
4.2.3.1	Ensure changes to system administration scope (sudoers) is collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.2.3.2	Ensure actions as another user are always logged (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.3	Ensure events that modify the sudo log file are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.4	Ensure events that modify date and time information are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.5	Ensure events that modify the system's network environment are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.6	Ensure use of privileged commands are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.7	Ensure unsuccessful file access attempts are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.8	Ensure events that modify user/group information are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.9	Ensure discretionary access control permission modification events are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.10	Ensure successful file system mounts are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.11	Ensure session initiation information is collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.12	Ensure login and logout events are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.13	Ensure file deletion events by users are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.14	Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.2.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.19	Ensure kernel module loading unloading and modification is collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.20	Ensure the audit configuration is immutable (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3.21	Ensure the running and on disk configuration is the same (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	Configure auditd file access		
4.2.4.1	Ensure audit log files are mode 0600 or less permissive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4.2	Ensure only authorized users own audit log files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4.3	Ensure only authorized groups are assigned ownership of audit log files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4.4	Ensure the audit log directory is 0750 or more restrictive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4.5	Ensure audit configuration files are 640 or more restrictive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4.6	Ensure audit configuration files are owned by root (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4.7	Ensure audit configuration files belong to group root (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4.8	Ensure audit tools are 755 or more restrictive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.2.4.9	Ensure audit tools are owned by root (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4.10	Ensure audit tools belong to group root (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4.11	Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)	<input type="checkbox"/>	<input 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 type="checkbox"/>
5.1.2	Ensure permissions on /etc/crontab are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure permissions on /etc/cron.daily are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure permissions on /etc/cron.d are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.8	Ensure cron is restricted to authorized users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.9	Ensure at is restricted to authorized users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Configure SSH Server		
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2.2	Ensure permissions on SSH private host key files are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure permissions on SSH public host key files are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure SSH access is limited (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure SSH LogLevel is appropriate (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure SSH PAM is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure SSH root login is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	Ensure SSH HostbasedAuthentication is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	Ensure SSH PermitEmptyPasswords is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	Ensure SSH PermitUserEnvironment is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	Ensure SSH IgnoreRhosts is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	Ensure SSH X11 forwarding is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	Ensure only strong Ciphers are used (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.14	Ensure only strong MAC algorithms are used (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.15	Ensure only strong Key Exchange algorithms are used (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.16	Ensure SSH AllowTcpForwarding is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.17	Ensure system-wide crypto policy is not over-ridden (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.18	Ensure SSH warning banner is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2.19	Ensure SSH MaxAuthTries is set to 4 or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.20	Ensure SSH MaxStartups is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.21	Ensure SSH MaxSessions is set to 10 or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.22	Ensure SSH LoginGraceTime is set to one minute or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.23	Ensure SSH Idle Timeout Interval is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3	Configure privilege escalation		
5.3.1	Ensure sudo is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2	Ensure sudo commands use pty (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	Ensure sudo log file exists (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.4	Ensure users must provide password for privilege escalation (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.5	Ensure re-authentication for privilege escalation is not disabled globally (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.6	Ensure sudo authentication timeout is configured correctly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.7	Ensure access to the su command is restricted (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 lockout for failed password attempts is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.4.3	Ensure password reuse is limited (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.4	Ensure password hashing algorithm is up to date with the latest standards (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.5	Ensure all current passwords uses the configured hashing algorithm (Manual)	<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 warning days is 7 or more (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.4	Ensure inactive password lock is 30 days or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1.5	Ensure all users last password change date is in the past (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.2	Ensure system accounts are secured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5.3	Ensure default 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 shell timeout is 900 seconds or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6	System Maintenance		
6.1	System File Permissions		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.1.1	Ensure permissions on /etc/passwd are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure permissions on /etc/passwd- are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Ensure permissions on /etc/group are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.4	Ensure permissions on /etc/group- are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.5	Ensure permissions on /etc/shadow are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.6	Ensure permissions on /etc/shadow- are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.7	Ensure permissions on /etc/gshadow are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.8	Ensure permissions on /etc/gshadow- are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.9	Ensure no world writable files exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.10	Ensure no unowned files or directories exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.11	Ensure no ungrouped files or directories exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.12	Audit SUID executables (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.13	Audit SGID executables (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.2	Local 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 /etc/shadow password fields are not empty (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.2.3	Ensure all groups in /etc/passwd exist in /etc/group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Ensure shadow group is empty (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure no duplicate UIDs exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure no duplicate GIDs exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure no duplicate user names exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure no duplicate group names exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.9	Ensure root PATH Integrity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.10	Ensure root is the only UID 0 account (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.11	Ensure local interactive user home directories exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.12	Ensure local interactive users own their home directories (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.13	Ensure local interactive user home directories are mode 750 or more restrictive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.14	Ensure no local interactive user has .netrc files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.15	Ensure no local interactive user has .forward files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.16	Ensure no local interactive user has .rhosts files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.17	Ensure local interactive user dot files are not group or world writable (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
Jul 18, 2022	1.0.0	Draft Published for consensus review

DRAFT