



# CIS Debian Linux 11 Benchmark

v2.0.0 - 03-29-2024

# Terms of Use

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

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

# Table of Contents

<b>Terms of Use .....</b>	<b>1</b>
<b>Table of Contents .....</b>	<b>2</b>
<b>Overview .....</b>	<b>11</b>
<b>Intended Audience.....</b>	<b>11</b>
<b>Consensus Guidance .....</b>	<b>12</b>
<b>Typographical Conventions.....</b>	<b>13</b>
<b>Recommendation Definitions.....</b>	<b>14</b>
<b>Title .....</b>	<b>14</b>
<b>Assessment Status.....</b>	<b>14</b>
<b>Automated .....</b>	<b>14</b>
<b>Manual.....</b>	<b>14</b>
<b>Profile .....</b>	<b>14</b>
<b>Description.....</b>	<b>14</b>
<b>Rationale Statement .....</b>	<b>14</b>
<b>Impact Statement.....</b>	<b>15</b>
<b>Audit Procedure.....</b>	<b>15</b>
<b>Remediation Procedure.....</b>	<b>15</b>
<b>Default Value.....</b>	<b>15</b>
<b>References .....</b>	<b>15</b>
<b>CIS Critical Security Controls® (CIS Controls®) .....</b>	<b>15</b>
<b>Additional Information.....</b>	<b>15</b>
<b>Profile Definitions .....</b>	<b>16</b>
<b>Acknowledgements .....</b>	<b>17</b>
<b>Recommendations .....</b>	<b>18</b>
<b>1 Initial Setup .....</b>	<b>18</b>
<b>1.1 Filesystem .....</b>	<b>19</b>
<b>1.1.1 Configure Filesystem Kernel Modules .....</b>	<b>20</b>
1.1.1.1 Ensure cramfs kernel module is not available (Automated) .....	21
1.1.1.2 Ensure freevxfs kernel module is not available (Automated) .....	26
1.1.1.3 Ensure hfs kernel module is not available (Automated) .....	31
1.1.1.4 Ensure hfsplus kernel module is not available (Automated) .....	36
1.1.1.5 Ensure jffs2 kernel module is not available (Automated) .....	41
1.1.1.6 Ensure squashfs kernel module is not available (Automated) .....	46
1.1.1.7 Ensure udf kernel module is not available (Automated) .....	51
1.1.1.8 Ensure usb-storage kernel module is not available (Automated) .....	56
<b>1.1.2 Configure Filesystem Partitions .....</b>	<b>61</b>
<b>1.1.2.1 Configure /tmp .....</b>	<b>62</b>

1.1.2.1.1 Ensure /tmp is a separate partition (Automated) .....	63
1.1.2.1.2 Ensure nodev option set on /tmp partition (Automated) .....	67
1.1.2.1.3 Ensure nosuid option set on /tmp partition (Automated) .....	69
1.1.2.1.4 Ensure noexec option set on /tmp partition (Automated) .....	71
<b>1.1.2.2 Configure /dev/shm .....</b>	<b>73</b>
1.1.2.2.1 Ensure /dev/shm is a separate partition (Automated) .....	74
1.1.2.2.2 Ensure nodev option set on /dev/shm partition (Automated) .....	76
1.1.2.2.3 Ensure nosuid option set on /dev/shm partition (Automated) .....	78
1.1.2.2.4 Ensure noexec option set on /dev/shm partition (Automated) .....	80
<b>1.1.2.3 Configure /home .....</b>	<b>82</b>
1.1.2.3.1 Ensure separate partition exists for /home (Automated) .....	83
1.1.2.3.2 Ensure nodev option set on /home partition (Automated) .....	85
1.1.2.3.3 Ensure nosuid option set on /home partition (Automated) .....	87
<b>1.1.2.4 Configure /var .....</b>	<b>89</b>
1.1.2.4.1 Ensure separate partition exists for /var (Automated) .....	90
1.1.2.4.2 Ensure nodev option set on /var partition (Automated) .....	93
1.1.2.4.3 Ensure nosuid option set on /var partition (Automated) .....	95
<b>1.1.2.5 Configure /var/tmp .....</b>	<b>97</b>
1.1.2.5.1 Ensure separate partition exists for /var/tmp (Automated) .....	98
1.1.2.5.2 Ensure nodev option set on /var/tmp partition (Automated) .....	100
1.1.2.5.3 Ensure nosuid option set on /var/tmp partition (Automated) .....	102
1.1.2.5.4 Ensure noexec option set on /var/tmp partition (Automated) .....	104
<b>1.1.2.6 Configure /var/log .....</b>	<b>106</b>
1.1.2.6.1 Ensure separate partition exists for /var/log (Automated) .....	107
1.1.2.6.2 Ensure nodev option set on /var/log partition (Automated) .....	109
1.1.2.6.3 Ensure nosuid option set on /var/log partition (Automated) .....	111
1.1.2.6.4 Ensure noexec option set on /var/log partition (Automated) .....	113
<b>1.1.2.7 Configure /var/log/audit .....</b>	<b>115</b>
1.1.2.7.1 Ensure separate partition exists for /var/log/audit (Automated) .....	116
1.1.2.7.2 Ensure nodev option set on /var/log/audit partition (Automated) .....	118
1.1.2.7.3 Ensure nosuid option set on /var/log/audit partition (Automated) .....	120
1.1.2.7.4 Ensure noexec option set on /var/log/audit partition (Automated) .....	122
<b>1.2 Package Management .....</b>	<b>124</b>
<b>1.2.1 Configure Package Repositories .....</b>	<b>125</b>
1.2.1.1 Ensure GPG keys are configured (Manual) .....	126
1.2.1.2 Ensure package manager repositories are configured (Manual) .....	128
<b>1.2.2 Configure Package Updates .....</b>	<b>130</b>
1.2.2.1 Ensure updates, patches, and additional security software are installed (Manual) .....	131
<b>1.3 Mandatory Access Control .....</b>	<b>134</b>
<b>1.3.1 Configure AppArmor .....</b>	<b>135</b>
1.3.1.1 Ensure AppArmor is installed (Automated) .....	136
1.3.1.2 Ensure AppArmor is enabled in the bootloader configuration (Automated) .....	138
1.3.1.3 Ensure all AppArmor Profiles are in enforce or complain mode (Automated) .....	140
1.3.1.4 Ensure all AppArmor Profiles are enforcing (Automated) .....	142
<b>1.4 Configure Bootloader .....</b>	<b>144</b>
1.4.1 Ensure bootloader password is set (Automated) .....	145
1.4.2 Ensure access to bootloader config is configured (Automated) .....	148
<b>1.5 Configure Additional Process Hardening .....</b>	<b>150</b>
1.5.1 Ensure address space layout randomization is enabled (Automated) .....	151
1.5.2 Ensure ptrace_scope is restricted (Automated) .....	155
1.5.3 Ensure core dumps are restricted (Automated) .....	159
1.5.4 Ensure prelink is not installed (Automated) .....	162
1.5.5 Ensure Automatic Error Reporting is not enabled (Automated) .....	164
<b>1.6 Configure Command Line Warning Banners .....</b>	<b>166</b>
1.6.1 Ensure message of the day is configured properly (Automated) .....	167
1.6.2 Ensure local login warning banner is configured properly (Automated) .....	169

1.6.3 Ensure remote login warning banner is configured properly (Automated) .....	171
1.6.4 Ensure access to /etc/motd is configured (Automated) .....	173
1.6.5 Ensure access to /etc/issue is configured (Automated) .....	175
1.6.6 Ensure access to /etc/issue.net is configured (Automated) .....	177
<b>1.7 Configure GNOME Display Manager.....</b>	<b>179</b>
1.7.1 Ensure GDM is removed (Automated) .....	180
1.7.2 Ensure GDM login banner is configured (Automated) .....	182
1.7.3 Ensure GDM disable-user-list option is enabled (Automated) .....	186
1.7.4 Ensure GDM screen locks when the user is idle (Automated) .....	190
1.7.5 Ensure GDM screen locks cannot be overridden (Automated) .....	193
1.7.6 Ensure GDM automatic mounting of removable media is disabled (Automated).....	196
1.7.7 Ensure GDM disabling automatic mounting of removable media is not overridden (Automated) .....	202
1.7.8 Ensure GDM autorun-never is enabled (Automated) .....	205
1.7.9 Ensure GDM autorun-never is not overridden (Automated) .....	210
1.7.10 Ensure XDCMP is not enabled (Automated) .....	213
<b>2 Services.....</b>	<b>216</b>
<b>2.1 Configure Server Services .....</b>	<b>217</b>
2.1.1 Ensure autofs services are not in use (Automated).....	218
2.1.2 Ensure avahi daemon services are not in use (Automated).....	221
2.1.3 Ensure dhcp server services are not in use (Automated).....	224
2.1.4 Ensure dns server services are not in use (Automated).....	227
2.1.5 Ensure dhsmasq services are not in use (Automated).....	229
2.1.6 Ensure ftp server services are not in use (Automated) .....	232
2.1.7 Ensure ldap server services are not in use (Automated).....	235
2.1.8 Ensure message access server services are not in use (Automated) .....	238
2.1.9 Ensure network file system services are not in use (Automated).....	242
2.1.10 Ensure nis server services are not in use (Automated).....	245
2.1.11 Ensure print server services are not in use (Automated) .....	248
2.1.12 Ensure rpcbind services are not in use (Automated).....	251
2.1.13 Ensure rsync services are not in use (Automated).....	254
2.1.14 Ensure samba file server services are not in use (Automated).....	257
2.1.15 Ensure snmp services are not in use (Automated).....	260
2.1.16 Ensure tftp server services are not in use (Automated) .....	263
2.1.17 Ensure web proxy server services are not in use (Automated) .....	266
2.1.18 Ensure web server services are not in use (Automated) .....	269
2.1.19 Ensure xinetd services are not in use (Automated) .....	273
2.1.20 Ensure X window server services are not in use (Automated) .....	276
2.1.21 Ensure mail transfer agent is configured for local-only mode (Automated) .....	278
2.1.22 Ensure only approved services are listening on a network interface (Manual) .....	281
<b>2.2 Configure Client Services .....</b>	<b>284</b>
2.2.1 Ensure NIS Client is not installed (Automated) .....	285
2.2.2 Ensure rsh client is not installed (Automated) .....	287
2.2.3 Ensure talk client is not installed (Automated) .....	289
2.2.4 Ensure telnet client is not installed (Automated) .....	291
2.2.5 Ensure ldap client is not installed (Automated) .....	293
2.2.6 Ensure ftp client is not installed (Automated) .....	295
<b>2.3 Configure Time Synchronization .....</b>	<b>297</b>
<b>2.3.1 Ensure time synchronization is in use.....</b>	<b>298</b>
2.3.1.1 Ensure a single time synchronization daemon is in use (Automated).....	299
<b>2.3.2 Configure systemd-timesyncd.....</b>	<b>303</b>
2.3.2.1 Ensure systemd-timesyncd configured with authorized timeserver (Automated) .....	305
2.3.2.2 Ensure systemd-timesyncd is enabled and running (Manual).....	309
<b>2.3.3 Configure chrony .....</b>	<b>311</b>
2.3.3.1 Ensure chrony is configured with authorized timeserver (Manual).....	312

2.3.3.2 Ensure chrony is running as user _chrony (Automated) .....	316
2.3.3.3 Ensure chrony is enabled and running (Automated) .....	318
<b>2.4 Job Schedulers .....</b>	<b>320</b>
<b>2.4.1 Configure cron.....</b>	<b>321</b>
2.4.1.1 Ensure cron daemon is enabled and active (Automated) .....	322
2.4.1.2 Ensure permissions on /etc/crontab are configured (Automated) .....	324
2.4.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated) .....	326
2.4.1.4 Ensure permissions on /etc/cron.daily are configured (Automated).....	328
2.4.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated) .....	330
2.4.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated).....	332
2.4.1.7 Ensure permissions on /etc/cron.d are configured (Automated) .....	334
2.4.1.8 Ensure crontab is restricted to authorized users (Automated) .....	336
<b>2.4.2 Configure at .....</b>	<b>340</b>
2.4.2.1 Ensure at is restricted to authorized users (Automated) .....	341
<b>3 Network .....</b>	<b>345</b>
<b>3.1 Configure Network Devices .....</b>	<b>346</b>
3.1.1 Ensure IPv6 status is identified (Manual) .....	347
3.1.2 Ensure wireless interfaces are disabled (Automated).....	350
3.1.3 Ensure bluetooth services are not in use (Automated).....	354
<b>3.2 Configure Network Kernel Modules .....</b>	<b>357</b>
3.2.1 Ensure dccp kernel module is not available (Automated) .....	358
3.2.2 Ensure tipc kernel module is not available (Automated) .....	363
3.2.3 Ensure rds kernel module is not available (Automated).....	368
3.2.4 Ensure sctp kernel module is not available (Automated) .....	373
<b>3.3 Configure Network Kernel Parameters.....</b>	<b>378</b>
3.3.1 Ensure ip forwarding is disabled (Automated) .....	379
3.3.2 Ensure packet redirect sending is disabled (Automated) .....	383
3.3.3 Ensure bogus icmp responses are ignored (Automated) .....	387
3.3.4 Ensure broadcast icmp requests are ignored (Automated).....	391
3.3.5 Ensure icmp redirects are not accepted (Automated) .....	395
3.3.6 Ensure secure icmp redirects are not accepted (Automated) .....	399
3.3.7 Ensure reverse path filtering is enabled (Automated) .....	403
3.3.8 Ensure source routed packets are not accepted (Automated) .....	407
3.3.9 Ensure suspicious packets are logged (Automated) .....	412
3.3.10 Ensure tcp syn cookies is enabled (Automated) .....	416
3.3.11 Ensure ipv6 router advertisements are not accepted (Automated) .....	420
<b>4 Host Based Firewall.....</b>	<b>424</b>
<b>4.1 Configure UncomplicatedFirewall.....</b>	<b>425</b>
4.1.1 Ensure ufw is installed (Automated) .....	426
4.1.2 Ensure iptables-persistent is not installed with ufw (Automated) .....	428
4.1.3 Ensure ufw service is enabled (Automated) .....	430
4.1.4 Ensure ufw loopback traffic is configured (Automated) .....	433
4.1.5 Ensure ufw outbound connections are configured (Manual) .....	435
4.1.6 Ensure ufw firewall rules exist for all open ports (Automated) .....	437
4.1.7 Ensure ufw default deny firewall policy (Automated).....	440
<b>4.2 Configure nftables .....</b>	<b>442</b>
4.2.1 Ensure nftables is installed (Automated) .....	445
4.2.2 Ensure ufw is uninstalled or disabled with nftables (Automated) .....	447
4.2.3 Ensure iptables are flushed with nftables (Manual).....	449
4.2.4 Ensure a nftables table exists (Automated) .....	451
4.2.5 Ensure nftables base chains exist (Automated) .....	453
4.2.6 Ensure nftables loopback traffic is configured (Automated) .....	455
4.2.7 Ensure nftables outbound and established connections are configured (Manual).....	457
4.2.8 Ensure nftables default deny firewall policy (Automated).....	460
4.2.9 Ensure nftables service is enabled (Automated) .....	463

4.2.10 Ensure nftables rules are permanent (Automated).....	465
<b>4.3 Configure iptables .....</b>	<b>468</b>
<b>4.3.1 Configure iptables software .....</b>	<b>469</b>
4.3.1.1 Ensure iptables packages are installed (Automated) .....	470
4.3.1.2 Ensure nftables is not installed with iptables (Automated) .....	472
4.3.1.3 Ensure ufw is uninstalled or disabled with iptables (Automated) .....	474
<b>4.3.2 Configure IPv4 iptables .....</b>	<b>476</b>
4.3.2.1 Ensure iptables default deny firewall policy (Automated) .....	477
4.3.2.2 Ensure iptables loopback traffic is configured (Automated) .....	479
4.3.2.3 Ensure iptables outbound and established connections are configured (Manual)....	481
4.3.2.4 Ensure iptables firewall rules exist for all open ports (Automated).....	483
<b>4.3.3 Configure IPv6 ip6tables .....</b>	<b>486</b>
4.3.3.1 Ensure ip6tables default deny firewall policy (Automated) .....	487
4.3.3.2 Ensure ip6tables loopback traffic is configured (Automated) .....	490
4.3.3.3 Ensure ip6tables outbound and established connections are configured (Manual)...	493
4.3.3.4 Ensure ip6tables firewall rules exist for all open ports (Automated).....	495
<b>5 Access Control .....</b>	<b>498</b>
<b>5.1 Configure SSH Server .....</b>	<b>499</b>
5.1.1 Ensure permissions on /etc/ssh/sshd_config are configured (Automated) .....	501
5.1.2 Ensure permissions on SSH private host key files are configured (Automated) .....	504
5.1.3 Ensure permissions on SSH public host key files are configured (Automated) .....	508
5.1.4 Ensure sshd access is configured (Automated) .....	512
5.1.5 Ensure sshd Banner is configured (Automated).....	515
5.1.6 Ensure sshd Ciphers are configured (Automated) .....	517
5.1.7 Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured (Automated) .....	520
5.1.8 Ensure sshd DisableForwarding is enabled (Automated) .....	523
5.1.9 Ensure sshd GSSAPIAuthentication is disabled (Automated) .....	526
5.1.10 Ensure sshd HostbasedAuthentication is disabled (Automated).....	528
5.1.11 Ensure sshd IgnoreRhosts is enabled (Automated) .....	530
5.1.12 Ensure sshd KexAlgorithms is configured (Automated) .....	532
5.1.13 Ensure sshd LoginGraceTime is configured (Automated).....	535
5.1.14 Ensure sshd LogLevel is configured (Automated).....	537
5.1.15 Ensure sshd MACs are configured (Automated) .....	539
5.1.16 Ensure sshd MaxAuthTries is configured (Automated) .....	542
5.1.17 Ensure sshd MaxSessions is configured (Automated) .....	544
5.1.18 Ensure sshd MaxStartups is configured (Automated) .....	546
5.1.19 Ensure sshd PermitEmptyPasswords is disabled (Automated) .....	548
5.1.20 Ensure sshd PermitRootLogin is disabled (Automated) .....	550
5.1.21 Ensure sshd PermitUserEnvironment is disabled (Automated) .....	552
5.1.22 Ensure sshd UsePAM is enabled (Automated) .....	554
<b>5.2 Configure privilege escalation .....</b>	<b>556</b>
5.2.1 Ensure sudo is installed (Automated).....	557
5.2.2 Ensure sudo commands use pty (Automated) .....	559
5.2.3 Ensure sudo log file exists (Automated) .....	562
5.2.4 Ensure users must provide password for privilege escalation (Automated) .....	564
5.2.5 Ensure re-authentication for privilege escalation is not disabled globally (Automated)	566
5.2.6 Ensure sudo authentication timeout is configured correctly (Automated) .....	568
5.2.7 Ensure access to the su command is restricted (Automated) .....	570
<b>5.3 Pluggable Authentication Modules .....</b>	<b>572</b>
<b>5.3.1 Configure PAM software packages .....</b>	<b>573</b>
5.3.1.1 Ensure latest version of pam is installed (Automated) .....	574
5.3.1.2 Ensure libpam-modules is installed (Automated) .....	575
5.3.1.3 Ensure libpam-pwquality is installed (Automated).....	576
<b>5.3.2 Configure pam-auth-update profiles .....</b>	<b>577</b>

5.3.2.1 Ensure pam_unix module is enabled (Automated).....	578
5.3.2.2 Ensure pam_faillock module is enabled (Automated) .....	580
5.3.2.3 Ensure pam_pwquality module is enabled (Automated) .....	583
5.3.2.4 Ensure pam_pwhistory module is enabled (Automated) .....	586
<b>5.3.3 Configure PAM Arguments .....</b>	<b>589</b>
<b>5.3.3.1 Configure pam_faillock module .....</b>	<b>590</b>
5.3.3.1.1 Ensure password failed attempts lockout is configured (Automated).....	591
5.3.3.1.2 Ensure password unlock time is configured (Automated) .....	593
5.3.3.1.3 Ensure password failed attempts lockout includes root account (Automated) .....	596
<b>5.3.3.2 Configure pam_pwquality module .....</b>	<b>599</b>
5.3.3.2.1 Ensure password number of changed characters is configured (Automated) .....	601
5.3.3.2.2 Ensure minimum password length is configured (Automated) .....	605
5.3.3.2.3 Ensure password complexity is configured (Manual) .....	609
5.3.3.2.4 Ensure password same consecutive characters is configured (Automated).....	613
5.3.3.2.5 Ensure password maximum sequential characters is configured (Automated) .....	617
5.3.3.2.6 Ensure password dictionary check is enabled (Automated).....	621
5.3.3.2.7 Ensure password quality checking is enforced (Automated).....	624
5.3.3.2.8 Ensure password quality is enforced for the root user (Automated) .....	626
<b>5.3.3.3 Configure pam_pwhistory module .....</b>	<b>629</b>
5.3.3.3.1 Ensure password history remember is configured (Automated) .....	630
5.3.3.3.2 Ensure password history is enforced for the root user (Automated) .....	633
5.3.3.3.3 Ensure pam_pwhistory includes use_authok (Automated) .....	636
<b>5.3.3.4 Configure pam_unix module .....</b>	<b>638</b>
5.3.3.4.1 Ensure pam_unix does not include nullok (Automated) .....	639
5.3.3.4.2 Ensure pam_unix does not include remember (Automated) .....	642
5.3.3.4.3 Ensure pam_unix includes a strong password hashing algorithm (Automated) .....	644
5.3.3.4.4 Ensure pam_unix includes use_authok (Automated) .....	648
<b>5.4 User Accounts and Environment .....</b>	<b>651</b>
<b>5.4.1 Configure shadow password suite parameters .....</b>	<b>652</b>
5.4.1.1 Ensure password expiration is configured (Automated) .....	653
5.4.1.2 Ensure minimum password age is configured (Manual) .....	657
5.4.1.3 Ensure password expiration warning days is configured (Automated).....	660
5.4.1.4 Ensure strong password hashing algorithm is configured (Automated) .....	662
5.4.1.5 Ensure inactive password lock is configured (Automated) .....	665
5.4.1.6 Ensure all users last password change date is in the past (Automated).....	668
<b>5.4.2 Configure root and system accounts and environment .....</b>	<b>670</b>
5.4.2.1 Ensure root is the only UID 0 account (Automated) .....	671
5.4.2.2 Ensure root is the only GID 0 account (Automated).....	672
5.4.2.3 Ensure group root is the only GID 0 group (Automated) .....	674
5.4.2.4 Ensure root password is set (Automated) .....	676
5.4.2.5 Ensure root path integrity (Automated).....	678
5.4.2.6 Ensure root user umask is configured (Automated) .....	681
5.4.2.7 Ensure system accounts do not have a valid login shell (Automated) .....	684
5.4.2.8 Ensure accounts without a valid login shell are locked (Automated) .....	687
<b>5.4.3 Configure user default environment .....</b>	<b>689</b>
5.4.3.1 Ensure nologin is not listed in /etc/shells (Automated).....	690
5.4.3.2 Ensure default user shell timeout is configured (Automated) .....	691
5.4.3.3 Ensure default user umask is configured (Automated) .....	695
<b>6 Logging and Auditing.....</b>	<b>702</b>
<b>6.1 Configure Integrity Checking .....</b>	<b>703</b>
6.1.1 Ensure AIDE is installed (Automated) .....	704
6.1.2 Ensure filesystem integrity is regularly checked (Automated) .....	706
6.1.3 Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated) .....	709
<b>6.2 System Logging .....</b>	<b>712</b>

<b>6.2.1 Configure journald .....</b>	<b>713</b>
<b>6.2.1.1 Configure systemd-journald service .....</b>	<b>714</b>
6.2.1.1.1 Ensure journald service is enabled and active (Automated) .....	715
6.2.1.1.2 Ensure journald log file access is configured (Manual) .....	717
6.2.1.1.3 Ensure journald log file rotation is configured (Manual) .....	719
6.2.1.1.4 Ensure journald ForwardToSyslog is disabled (Automated) .....	721
6.2.1.1.5 Ensure journald Storage is configured (Automated).....	725
6.2.1.1.6 Ensure journald Compress is configured (Automated).....	729
<b>6.2.1.2 Configure systemd-journal-remote.....</b>	<b>733</b>
6.2.1.2.1 Ensure systemd-journal-remote is installed (Automated).....	734
6.2.1.2.2 Ensure systemd-journal-remote authentication is configured (Manual) .....	736
6.2.1.2.3 Ensure systemd-journal-upload is enabled and active (Automated) .....	738
6.2.1.2.4 Ensure systemd-journal-remote service is not in use (Automated).....	740
<b>6.2.2 Configure Logfiles.....</b>	<b>742</b>
6.2.2.1 Ensure access to all logfiles has been configured (Automated).....	743
<b>6.4 System Auditing.....</b>	<b>749</b>
<b>6.4.1 Configure auditd Service.....</b>	<b>751</b>
6.4.1.1 Ensure auditd packages are installed (Automated).....	752
6.4.1.2 Ensure auditd service is enabled and active (Automated) .....	754
6.4.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated) .....	756
6.4.1.4 Ensure audit_backlog_limit is sufficient (Automated) .....	758
<b>6.4.2 Configure Data Retention.....</b>	<b>760</b>
6.4.2.1 Ensure audit log storage size is configured (Automated).....	761
6.4.2.2 Ensure audit logs are not automatically deleted (Automated).....	763
6.4.2.3 Ensure system is disabled when audit logs are full (Automated) .....	765
6.4.2.4 Ensure system warns when audit logs are low on space (Automated).....	768
<b>6.4.3 Configure auditd Rules.....</b>	<b>771</b>
6.4.3.1 Ensure changes to system administration scope (sudoers) is collected (Automated)772	772
6.4.3.2 Ensure actions as another user are always logged (Automated).....	775
6.4.3.3 Ensure events that modify the sudo log file are collected (Automated) .....	779
6.4.3.4 Ensure events that modify date and time information are collected (Automated).....	783
6.4.3.5 Ensure events that modify the system's network environment are collected (Automated) .....	787
6.4.3.6 Ensure use of privileged commands are collected (Automated) .....	791
6.4.3.7 Ensure unsuccessful file access attempts are collected (Automated) .....	795
6.4.3.8 Ensure events that modify user/group information are collected (Automated) .....	799
6.4.3.9 Ensure discretionary access control permission modification events are collected (Automated) .....	803
6.4.3.10 Ensure successful file system mounts are collected (Automated) .....	808
6.4.3.11 Ensure session initiation information is collected (Automated) .....	812
6.4.3.12 Ensure login and logout events are collected (Automated) .....	816
6.4.3.13 Ensure file deletion events by users are collected (Automated) .....	819
6.4.3.14 Ensure events that modify the system's Mandatory Access Controls are collected (Automated) .....	823
6.4.3.15 Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated) .....	826
6.4.3.16 Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated) .....	830
6.4.3.17 Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated) .....	834
6.4.3.18 Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated) .....	838
6.4.3.19 Ensure kernel module loading unloading and modification is collected (Automated) .....	842
6.4.3.20 Ensure the audit configuration is immutable (Automated).....	846
6.4.3.21 Ensure the running and on disk configuration is the same (Manual) .....	849

<b>6.4.4 Configure auditd File Access.....</b>	<b>851</b>
6.4.4.1 Ensure audit log files mode is configured (Automated) .....	852
6.4.4.2 Ensure audit log files owner is configured (Automated) .....	855
6.4.4.3 Ensure audit log files group owner is configured (Automated) .....	858
6.4.4.4 Ensure the audit log file directory mode is configured (Automated) .....	860
6.4.4.5 Ensure audit configuration files mode is configured (Automated) .....	863
6.4.4.6 Ensure audit configuration files owner is configured (Automated) .....	865
6.4.4.7 Ensure audit configuration files group owner is configured (Automated) .....	867
6.4.4.8 Ensure audit tools mode is configured (Automated).....	869
6.4.4.9 Ensure audit tools owner is configured (Automated).....	872
6.4.4.10 Ensure audit tools group owner is configured (Automated) .....	874
<b>7 System Maintenance .....</b>	<b>876</b>
<b>    7.1 System File Permissions .....</b>	<b>877</b>
7.1.1 Ensure permissions on /etc/passwd are configured (Automated) .....	878
7.1.2 Ensure permissions on /etc/passwd- are configured (Automated).....	880
7.1.3 Ensure permissions on /etc/group are configured (Automated) .....	882
7.1.4 Ensure permissions on /etc/group- are configured (Automated).....	884
7.1.5 Ensure permissions on /etc/shadow are configured (Automated) .....	886
7.1.6 Ensure permissions on /etc/shadow- are configured (Automated).....	888
7.1.7 Ensure permissions on /etc/gshadow are configured (Automated).....	890
7.1.8 Ensure permissions on /etc/gshadow- are configured (Automated).....	892
7.1.9 Ensure permissions on /etc/shells are configured (Automated) .....	894
7.1.10 Ensure permissions on /etc/security/opasswd are configured (Automated) .....	896
7.1.11 Ensure world writable files and directories are secured (Automated) .....	898
7.1.12 Ensure no files or directories without an owner and a group exist (Automated) .....	902
7.1.13 Ensure SUID and SGID files are reviewed (Manual).....	905
<b>    7.2 Local User and Group Settings .....</b>	<b>908</b>
7.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated) .....	909
7.2.2 Ensure /etc/shadow password fields are not empty (Automated) .....	912
7.2.3 Ensure all groups in /etc/passwd exist in /etc/group (Automated) .....	914
7.2.4 Ensure shadow group is empty (Automated) .....	916
7.2.5 Ensure no duplicate UIDs exist (Automated).....	918
7.2.6 Ensure no duplicate GIDs exist (Automated) .....	919
7.2.7 Ensure no duplicate user names exist (Automated).....	921
7.2.8 Ensure no duplicate group names exist (Automated).....	923
7.2.9 Ensure local interactive user home directories are configured (Automated).....	925
7.2.10 Ensure local interactive user dot files access is configured (Automated) .....	930
<b>Appendix: Summary Table .....</b>	<b>936</b>
<b>Appendix: CIS Controls v7 IG 1 Mapped Recommendations .....</b>	<b>958</b>
<b>Appendix: CIS Controls v7 IG 2 Mapped Recommendations .....</b>	<b>964</b>
<b>Appendix: CIS Controls v7 IG 3 Mapped Recommendations .....</b>	<b>974</b>
<b>Appendix: CIS Controls v7 Unmapped Recommendations.....</b>	<b>984</b>
<b>Appendix: CIS Controls v8 IG 1 Mapped Recommendations .....</b>	<b>986</b>
<b>Appendix: CIS Controls v8 IG 2 Mapped Recommendations .....</b>	<b>993</b>
<b>Appendix: CIS Controls v8 IG 3 Mapped Recommendations .....</b>	<b>1003</b>
<b>Appendix: CIS Controls v8 Unmapped Recommendations.....</b>	<b>1013</b>
<b>Appendix: Change History .....</b>	<b>1015</b>



# 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 Debian Linux 11 systems running on x86\_64 platforms.

This guide was developed and tested against Debian Linux 11.9

The guidance within broadly assumes that operations are being performed as the `root` user, and executed under the default Bash version for the applicable distribution.

Operations performed using `sudo` instead of the `root` user, or executed under another shell, 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 default prompt for the `root` user is #, and as such all sample commands will have # as an additional indication that it is to be executed as `root`.

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](mailto: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 Debian Linux 11 on x86\_64 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/>.

# 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>&lt;italic font in brackets&gt;</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.
<b>Note</b>	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**

Ron Colvin  
Dave Billing  
Dominic Pace  
Koen Laevens  
Mark Birch  
Thomas Sjögren  
James Trigg  
Matthew Burkett  
Marcus Burghardt  
Graham Eames  
Robert McSulla  
Chad Streck  
Ryan Jaynes  
Tamas Tevesz  
Cory Sherman  
Simon John  
Nym Coy

### **Editor**

Jonathan Lewis Christopherson  
Eric Pinnell  
Justin Brown  
Gokhan Lus  
Randie Bejar

# **Recommendations**

## **1 Initial Setup**

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

## **1.1 Filesystem**

The file system is generally a built-in layer used to handle the data management of the storage.

### **1.1.1 Configure Filesystem Kernel Modules**

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 `/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**

Using `/bin/false` as the command in disabling a particular module serves 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 cramfs kernel module is not available (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 script to verify the `cramfs` module is disabled:

**-IF-** the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

**-IF-** available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
    l_mname="cramfs" # set module name
    l_mttype="fs" # set module type
    l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
    l_mpath="/lib/modules/**/kernel/$l_mttype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable=$(grep -P --
"(\^h*install\b\$l_mname\b)" <<< "$l_loadable")
        if grep -Pq -- '^h*install \/bin/(true|false)' <<< "$l_loadable"; then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
        fi
    }
    module_loaded_chk()
    {
        # Check if the module is currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
    }
    module_deny_chk()
    {
        # Check if the module is deny listed
        l_dl="y"
        if modprobe --showconfig | grep -Pq -- '^h*blacklist\b+'$l_mpname'\b'; then
            l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\b\$l_mname\b" $l_searchloc)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            l_output3="$l_output3\n - \"$l_mdir\""
            [ "$l_dl" != "y" ] && module_deny_chk
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mttype" ]; then
                module_loadable_chk
                module_loaded_chk
            fi
        else
            l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
        fi
    done
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_output3" ] && echo -e "\n\n-- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
    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:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

Run the following script to disable the `cramfs` module:

**-IF-** the module is available in the running kernel:

- Create a file ending in `.conf` with `install cramfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist cramfs` in the `/etc/modprobe.d/` directory
- Unload `cramfs` from the kernel

**-IF-** available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist cramfs` in the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```

#!/usr/bin/env bash

{
    l_mname="cramfs" # set module name
    l_mtype="fs" # set module type
    l_mpath="/lib/modules/**/kernel/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_fix()
    {
        # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
        #/etc/modprobe.d
        l_loadable=$(modprobe -n -v "$l_mname")
        [ $(wc -l <<< "$l_loadable") -gt "1" ] && l_loadable=$(grep -P --
        "(\^h*install|\b\$l_mname)\b" <<< "$l_loadable")
        if ! grep -Pq -- '\^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            echo -e "\n - setting module: \"$l_mname\" to be not loadable"
            echo -e "install \$l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    module_loaded_fix()
    {
        # If the module is currently loaded, unload the module
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e "\n - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
    }
    module_deny_fix()
    {
        # If the module isn't deny listed, denylist the module
        if ! modprobe --showconfig | grep -Pq -- "\^h*blacklist\h+\$l_mpname\b"; then
            echo -e "\n - deny listing \"$l_mname\""
            echo -e "blacklist \$l_mname" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/\$l_mndir" ] && [ -n "$(ls -A \$l_mdir/\$l_mndir)" ]; then
            echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
            module_deny_fix
            if [ "\$l_mdir" = "/lib/modules/$(uname -r)/kernel/\$l_mtype" ]; then
                module_loadable_fix
                module_loaded_fix
            fi
        else
            echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
        fi
    done
    echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}

```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

### *1.1.1.2 Ensure freevxfs kernel module is not available (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Run the following script to verify the `freevxfs` module is disabled:

**-IF-** the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

**-IF-** available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
    l_mname="freevxfs" # set module name
    l_mttype="fs" # set module type
    l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
    l_mpath="/lib/modules/**/kernel/$l_mttype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '_' <<< "$l_mname")
    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$l_loadable" = "0" ] && l_loadable=$(grep -P --
"^(^h*install\b\$l_mname\b)" <<< "$l_loadable")
        if grep -Pq -- '^h*install \/bin/(true|false)' <<< "$l_loadable"; then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
        fi
    }
    module_loaded_chk()
    {
        # Check if the module is currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
    }
    module_deny_chk()
    {
        # Check if the module is deny listed
        l_dl="y"
        if modprobe --showconfig | grep -Pq -- '^h*blacklist\b+'$l_mpname'\b'; then
            l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\b\$l_mname\b" $l_searchloc)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            l_output3="$l_output3\n - \"$l_mdir\""
            [ "$l_dl" != "y" ] && module_deny_chk
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mttype" ]; then
                module_loadable_chk
                module_loaded_chk
            fi
        else
            l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
        fi
    done
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_output3" ] && echo -e "\n\n-- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
    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:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

Run the following script to disable the `freevxfs` module:

**-IF-** the module is available in the running kernel:

- Create a file ending in `.conf` with `install freevxfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist freevxfs` in the `/etc/modprobe.d/` directory
- Unload `freevxfs` from the kernel

**-IF-** available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist freevxfs` in the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```

#!/usr/bin/env bash

{
    l_mname="freevxfs" # set module name
    l_mtype="fs" # set module type
    l_mpath="/lib/modules/**/kernel/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_fix()
    {
        # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
        #/etc/modprobe.d
        l_loadable=$(modprobe -n -v "$l_mname")
        [ $(wc -l <<< "$l_loadable") -gt "1" ] && l_loadable=$(grep -P --
        "(\^h*install|\b\$l_mname)\b" <<< "$l_loadable")
        if ! grep -Pq -- '\^h*install \/bin\/(true|false)' <<< "$l_loadable"; then
            echo -e "\n - setting module: \"$l_mname\" to be not loadable"
            echo -e "install \$l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    module_loaded_fix()
    {
        # If the module is currently loaded, unload the module
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e "\n - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
    }
    module_deny_fix()
    {
        # If the module isn't deny listed, denylist the module
        if ! modprobe --showconfig | grep -Pq -- "\^h*blacklist\h+\$l_mpname\b"; then
            echo -e "\n - deny listing \"$l_mname\""
            echo -e "blacklist \$l_mname" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/\$l_mndir" ] && [ -n "$(ls -A \$l_mdir/\$l_mndir)" ]; then
            echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
            module_deny_fix
            if [ "\$l_mdir" = "/lib/modules/$(uname -r)/kernel/\$l_mtype" ]; then
                module_loadable_fix
                module_loaded_fix
            fi
        else
            echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
        fi
    done
    echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}

```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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 hfs kernel module is not available (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Run the following script to verify the `hfs` module is disabled:

**-IF-** the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

**-IF-** available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
    l_mname="hfs" # set module name
    l_mttype="fs" # set module type
    l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
    l_mpath="/lib/modules/**/kernel/$l_mttype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable=$(grep -P --
"^(h*install\b\$l_mname\b)" <<< "$l_loadable")
        if grep -Pq -- '^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
        fi
    }
    module_loaded_chk()
    {
        # Check if the module is currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
    }
    module_deny_chk()
    {
        # Check if the module is deny listed
        l_dl="y"
        if modprobe --showconfig | grep -Pq -- '^h*blacklist\b+'$l_mpname'\b'; then
            l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\b\$l_mname\b" $l_searchloc)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            l_output3="$l_output3\n - \"$l_mdir\""
            [ "$l_dl" != "y" ] && module_deny_chk
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mttype" ]; then
                module_loadable_chk
                module_loaded_chk
            fi
        else
            l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
        fi
    done
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_output3" ] && echo -e "\n\n-- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
    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:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

Run the following script to disable the `hfs` module:

**-IF-** the module is available in the running kernel:

- Create a file ending in `.conf` with `install hfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist hfs` in the `/etc/modprobe.d/` directory
- Unload `hfs` from the kernel

**-IF-** available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist hfs` in the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```

#!/usr/bin/env bash

{
    l_mname="hfs" # set module name
    l_mtype="fs" # set module type
    l_mpath="/lib/modules/**/kernel/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_fix()
    {
        # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
        #/etc/modprobe.d
        l_loadable=$(modprobe -n -v "$l_mname")
        [ $(wc -l <<< "$l_loadable") -gt "1" ] && l_loadable=$(grep -P --
        "(\^h*install|\b\$l_mname)\b" <<< "$l_loadable")
        if ! grep -Pq -- '\^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            echo -e "\n - setting module: \"$l_mname\" to be not loadable"
            echo -e "install \$l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    module_loaded_fix()
    {
        # If the module is currently loaded, unload the module
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e "\n - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
    }
    module_deny_fix()
    {
        # If the module isn't deny listed, denylist the module
        if ! modprobe --showconfig | grep -Pq -- "\^h*blacklist\h+\$l_mpname\b"; then
            echo -e "\n - deny listing \"$l_mname\""
            echo -e "blacklist \$l_mname" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/\$l_mndir" ] && [ -n "$(ls -A \$l_mdir/\$l_mndir)" ]; then
            echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
            module_deny_fix
            if [ "\$l_mdir" = "/lib/modules/$(uname -r)/kernel/\$l_mtype" ]; then
                module_loadable_fix
                module_loaded_fix
            fi
        else
            echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
        fi
    done
    echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}

```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b></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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b></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

#### *1.1.1.4 Ensure hfsplus kernel module is not available (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

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

##### **Rationale:**

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

##### **Audit:**

Run the following script to verify the `hfsplus` module is disabled:

**-IF-** the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

**-IF-** available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
    l_mname="hfsplus" # set module name
    l_mttype="fs" # set module type
    l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
    l_mpath="/lib/modules/**/kernel/$l_mttype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable=$(grep -P --
"^(h*install\b\$l_mname\b)" <<< "$l_loadable")
        if grep -Pq -- '^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
        fi
    }
    module_loaded_chk()
    {
        # Check if the module is currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
    }
    module_deny_chk()
    {
        # Check if the module is deny listed
        l_dl="y"
        if modprobe --showconfig | grep -Pq -- '^h*blacklist\b+'$l_mpname'\b'; then
            l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\b\$l_mname\b" $l_searchloc)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            l_output3="$l_output3\n - \"$l_mdir\""
            [ "$l_dl" != "y" ] && module_deny_chk
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mttype" ]; then
                module_loadable_chk
                module_loaded_chk
            fi
        else
            l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
        fi
    done
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_output3" ] && echo -e "\n\n-- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
    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:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

**Remediation:**

Run the following script to disable the `hfsplus` module:

-IF- the module is available in the running kernel:

- Create a file ending in `.conf` with `install hfsplus /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist hfsplus` in the `/etc/modprobe.d/` directory
- Unload `hfsplus` from the kernel

-IF- available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist hfsplus` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```

#!/usr/bin/env bash

{
    l_mname="hfsplus" # set module name
    l_mtype="fs" # set module type
    l_mpath="/lib/modules/**/kernel/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_fix()
    {
        # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
        #/etc/modprobe.d
        l_loadable=$(modprobe -n -v "$l_mname")
        [ $(wc -l <<< "$l_loadable") -gt "1" ] && l_loadable=$(grep -P --
        "(\^h*install|\b\$l_mname)\b" <<< "$l_loadable")
        if ! grep -Pq -- '\^h*install \/bin\/(true|false)' <<< "$l_loadable"; then
            echo -e "\n - setting module: \"$l_mname\" to be not loadable"
            echo -e "install \$l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    module_loaded_fix()
    {
        # If the module is currently loaded, unload the module
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e "\n - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
    }
    module_deny_fix()
    {
        # If the module isn't deny listed, denylist the module
        if ! modprobe --showconfig | grep -Pq -- "\^h*blacklist\h+\$l_mpname\b"; then
            echo -e "\n - deny listing \"$l_mname\""
            echo -e "blacklist \$l_mname" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/\$l_mndir" ] && [ -n "$(ls -A \$l_mdir/\$l_mndir)" ]; then
            echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
            module_deny_fix
            if [ "\$l_mdir" = "/lib/modules/$(uname -r)/kernel/\$l_mtype" ]; then
                module_loadable_fix
                module_loaded_fix
            fi
        else
            echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
        fi
    done
    echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}

```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

### *1.1.1.5 Ensure jffs2 kernel module is not available (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Run the following script to verify the `jffs2` module is disabled:

**-IF-** the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

**-IF-** available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
    l_mname="jffs2" # set module name
    l_mttype="fs" # set module type
    l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
    l_mpath="/lib/modules/**/kernel/$l_mttype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable=$(grep -P --
"(\^h*install\b\$l_mname\b)" <<< "$l_loadable")
        if grep -Pq -- '^h*install \/bin/(true|false)' <<< "$l_loadable"; then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
        fi
    }
    module_loaded_chk()
    {
        # Check if the module is currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
    }
    module_deny_chk()
    {
        # Check if the module is deny listed
        l_dl="y"
        if modprobe --showconfig | grep -Pq -- '^h*blacklist\b+'$l_mpname'\b'; then
            l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\b\$l_mname\b" $l_searchloc)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            l_output3="$l_output3\n - \"$l_mdir\""
            [ "$l_dl" != "y" ] && module_deny_chk
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mttype" ]; then
                module_loadable_chk
                module_loaded_chk
            fi
        else
            l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
        fi
    done
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_output3" ] && echo -e "\n\n-- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
    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:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

Run the following script to disable the `jffs2` module:

**-IF-** the module is available in the running kernel:

- Create a file ending in `.conf` with `install jffs2 /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist jffs2` in the `/etc/modprobe.d/` directory
- Unload `jffs2` from the kernel

**-IF-** available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist jffs2` in the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```

#!/usr/bin/env bash

{
    l_mname="jffs2" # set module name
    l_mtype="fs" # set module type
    l_mpath="/lib/modules/**/kernel/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_fix()
    {
        # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
        #/etc/modprobe.d
        l_loadable=$(modprobe -n -v "$l_mname")
        [ $(wc -l <<< "$l_loadable") -gt "1" ] && l_loadable=$(grep -P --
        "(\^h*install|\b\$l_mname)\b" <<< "$l_loadable")
        if ! grep -Pq -- '\^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            echo -e "\n - setting module: \"$l_mname\" to be not loadable"
            echo -e "install \$l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    module_loaded_fix()
    {
        # If the module is currently loaded, unload the module
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e "\n - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
    }
    module_deny_fix()
    {
        # If the module isn't deny listed, denylist the module
        if ! modprobe --showconfig | grep -Pq -- "\^h*blacklist\h+\$l_mpname\b"; then
            echo -e "\n - deny listing \"$l_mname\""
            echo -e "blacklist \$l_mname" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/\$l_mndir" ] && [ -n "$(ls -A \$l_mdir/\$l_mndir)" ]; then
            echo -e "\n - module: \"$l_mname\" exists in \"\$l_mdir\"\n - checking if disabled..."
            module_deny_fix
            if [ "\$l_mdir" = "/lib/modules/$(uname -r)/kernel/\$l_mtype" ]; then
                module_loadable_fix
                module_loaded_fix
            fi
        else
            echo -e "\n - module: \"$l_mname\" doesn't exist in \"\$l_mdir\"\n"
        fi
    done
    echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}

```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b></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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b></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

## *1.1.1.6 Ensure squashfs kernel module is not available (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 script to verify the `squashfs` module is disabled:

**-IF-** the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

**-IF-** available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
    l_mname="squashfs" # set module name
    l_mttype="fs" # set module type
    l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
    l_mpath="/lib/modules/**/kernel/$l_mttype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable=$(grep -P --
"(\^h*install\b\$l_mname\b)" <<< "$l_loadable")
        if grep -Pq -- '^h*install \/bin/(true|false)' <<< "$l_loadable"; then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
        fi
    }
    module_loaded_chk()
    {
        # Check if the module is currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
    }
    module_deny_chk()
    {
        # Check if the module is deny listed
        l_dl="y"
        if modprobe --showconfig | grep -Pq -- '^h*blacklist\b+'$l_mpname'\b'; then
            l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\b\$l_mname\b" $l_searchloc)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            l_output3="$l_output3\n - \"$l_mdir\""
            [ "$l_dl" != "y" ] && module_deny_chk
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mttype" ]; then
                module_loadable_chk
                module_loaded_chk
            fi
        else
            l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
        fi
    done
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_output3" ] && echo -e "\n\n-- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
    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:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

**Note:** On operating systems where `squashfs` is pre-build into the kernel:

- This is considered an acceptable "passing" state
- The kernel **should not** be re-compiled to remove `squashfs`
- This audit will return as passing state with "module: "squashfs" doesn't exist in ..."

### **Remediation:**

Run the following script to disable the `squashfs` module:

-IF- the module is available in the running kernel:

- Create a file ending in `.conf` with `install squashfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist squashfs` in the `/etc/modprobe.d/` directory
- Unload `squashfs` from the kernel

-IF- available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist squashfs` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```

#!/usr/bin/env bash

{
    l_mname="squashfs" # set module name
    l_mtype="fs" # set module type
    l_mpath="/lib/modules/**/kernel/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_fix()
    {
        # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
        #/etc/modprobe.d
        l_loadable=$(modprobe -n -v "$l_mname")
        [ $(wc -l <<< "$l_loadable") -gt "1" ] && l_loadable=$(grep -P --
        "(\^h*install|\b\$l_mname)\b" <<< "$l_loadable")
        if ! grep -Pq -- '\^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            echo -e "\n - setting module: \"$l_mname\" to be not loadable"
            echo -e "install \$l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    module_loaded_fix()
    {
        # If the module is currently loaded, unload the module
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e "\n - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
    }
    module_deny_fix()
    {
        # If the module isn't deny listed, denylist the module
        if ! modprobe --showconfig | grep -Pq -- "\^h*blacklist\h+\$l_mpname\b"; then
            echo -e "\n - deny listing \"$l_mname\""
            echo -e "blacklist \$l_mname" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/\$l_mndir" ] && [ -n "$(ls -A \$l_mdir/\$l_mndir)" ]; then
            echo -e "\n - module: \"$l_mname\" exists in \"\$l_mdir\"\n - checking if disabled..."
            module_deny_fix
            if [ "\$l_mdir" = "/lib/modules/$(uname -r)/kernel/\$l_mtype" ]; then
                module_loadable_fix
                module_loaded_fix
            fi
        else
            echo -e "\n - module: \"$l_mname\" doesn't exist in \"\$l_mdir\"\n"
        fi
    done
    echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}

```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b></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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b></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

### *1.1.1.7 Ensure udf kernel module is not available (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 script to verify the `udf` module is disabled:

**-IF-** the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

**-IF-** available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
    l_mname="udf" # set module name
    l_mttype="fs" # set module type
    l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
    l_mpath="/lib/modules/**/kernel/$l_mttype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable=$(grep -P --
"^(h*install\b\$l_mname\b)" <<< "$l_loadable")
        if grep -Pq -- '^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
        fi
    }
    module_loaded_chk()
    {
        # Check if the module is currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
    }
    module_deny_chk()
    {
        # Check if the module is deny listed
        l_dl="y"
        if modprobe --showconfig | grep -Pq -- '^h*blacklist\b+'$l_mpname'\b'; then
            l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\b\$l_mname\b" $l_searchloc)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            l_output3="$l_output3\n - \"$l_mdir\""
            [ "$l_dl" != "y" ] && module_deny_chk
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mttype" ]; then
                module_loadable_chk
                module_loaded_chk
            fi
        else
            l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
        fi
    done
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_output3" ] && echo -e "\n\n-- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
    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:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

Run the following script to disable the `udf` module:

**-IF-** the module is available in the running kernel:

- Create a file ending in `.conf` with `install udf /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist udf` in the `/etc/modprobe.d/` directory
- Unload `udf` from the kernel

**-IF-** available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist udf` in the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```

#!/usr/bin/env bash

{
    l_mname="udf" # set module name
    l_mtype="fs" # set module type
    l_mpath="/lib/modules/**/kernel/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_fix()
    {
        # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
        #/etc/modprobe.d
        l_loadable=$(modprobe -n -v "$l_mname")
        [ $(wc -l <<< "$l_loadable") -gt "1" ] && l_loadable=$(grep -P --
        "(\^h*install|\b\$l_mname)\b" <<< "$l_loadable")
        if ! grep -Pq -- '\^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            echo -e "\n - setting module: \"$l_mname\" to be not loadable"
            echo -e "install \$l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    module_loaded_fix()
    {
        # If the module is currently loaded, unload the module
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e "\n - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
    }
    module_deny_fix()
    {
        # If the module isn't deny listed, denylist the module
        if ! modprobe --showconfig | grep -Pq -- "\^h*blacklist\h+\$l_mpname\b"; then
            echo -e "\n - deny listing \"$l_mname\""
            echo -e "blacklist \$l_mname" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/\$l_mndir" ] && [ -n "$(ls -A \$l_mdir/\$l_mndir)" ]; then
            echo -e "\n - module: \"$l_mname\" exists in \"\$l_mdir\"\n - checking if disabled..."
            module_deny_fix
            if [ "\$l_mdir" = "/lib/modules/$(uname -r)/kernel/\$l_mtype" ]; then
                module_loadable_fix
                module_loaded_fix
            fi
        else
            echo -e "\n - module: \"$l_mname\" doesn't exist in \"\$l_mdir\"\n"
        fi
    done
    echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}

```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b></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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b></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

### **1.1.1.8 Ensure usb-storage kernel module is not available (Automated)**

#### **Profile Applicability:**

- Level 1 - Server
- Level 2 - Workstation

#### **Description:**

USB storage provides a means to transfer and store files ensuring 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.

#### **Impact:**

Disabling the `usb-storage` module will disable any usage of USB storage devices.

If requirements and local site policy allow the use of such devices, other solutions should be configured accordingly instead. One example of a commonly used solution is `USBGuard`.

#### **Audit:**

Run the following script to verify the `usb-storage` module is disabled:

**-IF-** the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

**-IF-** available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system or pre-compiled into the kernel:

- No additional configuration is necessary

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
    l_mname="usb-storage" # set module name
    l_mttype="drivers" # set module type
    l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
    l_mpath="/lib/modules/**/kernel/$l_mttype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable=$(grep -P --
"^(h*install\b\$l_mname\b)" <<< "$l_loadable")
        if grep -Pq -- '^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
        fi
    }
    module_loaded_chk()
    {
        # Check if the module is currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
    }
    module_deny_chk()
    {
        # Check if the module is deny listed
        l_dl="y"
        if modprobe --showconfig | grep -Pq -- '^h*blacklist\b+'$l_mpname'\b'; then
            l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\b\$l_mname\b" $l_searchloc)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            l_output3="$l_output3\n - \"$l_mdir\""
            [ "$l_dl" != "y" ] && module_deny_chk
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mttype" ]; then
                module_loadable_chk
                module_loaded_chk
            fi
        else
            l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
        fi
    done
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_output3" ] && echo -e "\n\n-- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
    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:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

Run the following script to disable the `usb-storage` module:

**-IF-** the module is available in the running kernel:

- Create a file ending in `.conf` with `install usb-storage /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist usb-storage` in the `/etc/modprobe.d/` directory
- Unload `usb-storage` from the kernel

**-IF-** available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist usb-storage` in the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```

#!/usr/bin/env bash

{
    l_mname="usb-storage" # set module name
    l_mtype="drivers" # set module type
    l_mpath="/lib/modules/**/kernel/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_fix()
    {
        # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
        # /etc/modprobe.d
        l_loadable=$(modprobe -n -v "$l_mname")
        [ $(wc -l <<< "$l_loadable") -gt "1" ] && l_loadable=$(grep -P --
        "(\^h*install|\b\$l_mname)\b" <<< "$l_loadable")
        if ! grep -Pq -- '\^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            echo -e "\n - setting module: \"$l_mname\" to be not loadable"
            echo -e "install \$l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    module_loaded_fix()
    {
        # If the module is currently loaded, unload the module
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e "\n - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
    }
    module_deny_fix()
    {
        # If the module isn't deny listed, denylist the module
        if ! modprobe --showconfig | grep -Pq -- '\^h*blacklist\h+\$l_mpname\b'; then
            echo -e "\n - deny listing \"$l_mname\""
            echo -e "blacklist \$l_mname" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/\$l_mndir" ] && [ -n "$(ls -A \$l_mdir/\$l_mndir)" ]; then
            echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
            module_deny_fix
            if [ "\$l_mdir" = "/lib/modules/$(uname -r)/kernel/\$l_mtype" ]; then
                module_loadable_fix
                module_loaded_fix
            fi
        else
            echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
        fi
    done
    echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}

```

## References:

1. NIST SP 800-53 Rev. 5: SI-3

## Additional Information:

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

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

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>10.3 Disable Autorun and Autoplay for Removable Media</b> Disable autorun and autoplay auto-execute functionality for removable media.</p>	●	●	●
v7	<p><b>13.7 Manage USB Devices</b> If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.</p>		●	●

## MITRE ATT&CK Mappings:

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

## 1.1.2 Configure Filesystem Partitions

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 (This may require the system to be in single-user mode):

- Mount the new partition to a temporary mountpoint e.g. `mount /dev/sda2 /mnt`
- Copy data from the original partition to the new partition. e.g. `cp -a /var/tmp/* /mnt`
- Verify that all data is present on the new partition. e.g. `ls -la /mnt`
- Unmount the new partition. e.g. `umount /mnt`
- Remove the data from the original directory that was in the old partition. e.g. `rm -rf /var/tmp/*` Otherwise it will still consume space in the old partition that will be masked when the new filesystem is mounted.
- Mount the new partition to the desired mountpoint. e.g. `mount /dev/sda2 /var/tmp`
- Update `/etc/fstab` with the new mountpoint. e.g. `/dev/sda2 /var/tmp xfs defaults,rw,nosuid,nodev,noexec,relatime 0 0`

### **1.1.2.1 Configure /tmp**

The `/tmp` directory is a world-writable directory used to store data used by the system and user applications for a short period of time. This data should have no expectation of surviving a reboot, as this directory is intended to be emptied after each reboot.

### *1.1.2.1.1 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.

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

**Note:** In an environment where the main system is diskless and connected to iSCSI, entries in `/etc/fstab` may not take precedence.

`/tmp` can be configured to use `tmpfs`.

`tmpfs` puts everything into the kernel internal caches and grows and shrinks to accommodate the files it contains and is able to swap unneeded pages out to swap space. It has maximum size limits which can be adjusted on the fly via `mount -o remount`.

Since `tmpfs` lives completely in the page cache and on swap, all `tmpfs` pages will be shown as "Shmem" in `/proc/meminfo` and "Shared" in `free`. Notice that these counters also include shared memory. The most reliable way to get the count is using `df` and `du`.

`tmpfs` has three mount options for sizing:

- `size`: The limit of allocated bytes for this `tmpfs` instance. The default is half of your physical RAM without swap. If you oversize your `tmpfs` instances the machine will deadlock since the OOM handler will not be able to free that memory.
- `nr_blocks`: The same as `size`, but in blocks of `PAGE_SIZE`.
- `nr_inodes`: The maximum number of inodes for this instance. The default is half of the number of your physical RAM pages, or (on a machine with highmem) the number of lowmem RAM pages, whichever is the lower.

These parameters accept a suffix k, m or g and can be changed on remount. The `size` parameter also accepts a suffix % to limit this `tmpfs` instance to that percentage of your physical RAM. The default, when neither `size` nor `nr_blocks` is specified, is `size=50%`.

## 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:

By design files saved to `/tmp` should have no expectation of surviving a reboot of the system. `tmpfs` is ram based and all files stored to `tmpfs` will be lost when the system is rebooted.

If files need to be persistent through a reboot, they should be saved to `/var/tmp` not `/tmp`.

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

## 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 -kn /tmp
```

*Example output:*

```
/tmp    tmpfs    tmpfs    rw,nosuid,nodev,noexec
```

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

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

*Example output:*

```
generated
```

Verify output is not masked or disabled.

**Note:** 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`.

**Example of using `tmpfs` with specific mount options:**

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

**Note:** the `size=2G` is an example of setting a specific size for `tmpfs`.

Example of using a volume or disk with specific mount options. The source location of the volume or disk will vary depending on your environment:

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

## References:

1. <https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/>
2. <https://www.freedesktop.org/software/systemd/man/systemd-fstab-generator.html>
3. <https://www.kernel.org/doc/Documentation/filesystems/tmpfs.txt>
4. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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
T1499, T1499.001	TA0005	M1022

### *1.1.2.1.2 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:**

- **IF** - a separate partition exists for `/tmp`, verify that the `nodev` option is set.

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

*Example:*

```
# findmnt -kn /tmp | grep -v nodev  
Nothing should be returned
```

#### **Remediation:**

- **IF** - a separate partition exists for `/tmp`.

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.
2. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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
T1200, T1200.000	TA0005	M1022

### *1.1.2.1.3 Ensure nosuid option set on /tmp partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

- IF - a separate partition exists for `/tmp`, verify that the `nosuid` option is set.

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

Example:

```
# findmnt -kn /tmp | grep -v nosuid
```

```
Nothing should be returned
```

#### **Remediation:**

- IF - a separate partition exists for `/tmp`.

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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1548, T1548.001	TA0005	M1022

#### *1.1.2.1.4 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`.

##### **Impact:**

Setting the `noexec` option on `/tmp` may prevent installation and/or updating of some 3rd party software.

##### **Audit:**

- **IF** - a separate partition exists for `/tmp`, verify that the `noexec` option is set.

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

Example:

```
# findmnt -kn /tmp | grep -v noexec  
Nothing should be returned
```

##### **Remediation:**

- **IF** - a separate partition exists for `/tmp`.

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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1204, T1204.002	TA0005	M1022

### **1.1.2.2 Configure /dev/shm**

The `/dev/shm` directory is a world-writable directory that can function as shared memory that facilitates inter process communication (IPC)

### *1.1.2.2.1 Ensure /dev/shm is a separate partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `/dev/shm` directory is a world-writable directory that can function as shared memory that facilitates inter process communication (IPC).

#### **Rationale:**

Making `/dev/shm` its own file system allows an administrator to set additional mount options such as the `noexec` option on the mount, making `/dev/shm` useless for an attacker to install executable code. It would also prevent an attacker from establishing a 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 mounting `tmpfs` to `/dev/shm`.

#### **Impact:**

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

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

#### **Audit:**

**-IF-** `/dev/shm` is to be used on the system, run the following command and verify the output shows that `/dev/shm` is mounted. Particular requirements pertaining to mount options are covered in ensuing sections.

```
# findmnt -kn /dev/shm
```

#### *Example output:*

```
/dev/shm    tmpfs    tmpfs    rw,nosuid,nodev,noexec,relatime,seclabel
```

## **Remediation:**

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

*Example:*

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

## **References:**

1. <https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/>
2. <https://www.freedesktop.org/software/systemd/man/systemd-fstab-generator.html>
3. NIST SP 800-53 Rev. 5: CM-7

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> 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	TA0005	M1022

## *1.1.2.2 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:**

- **IF** - a separate partition exists for `/dev/shm`, verify that the `nodev` option is set.

```
# findmnt -kn /dev/shm | grep -v 'nodev'  
Nothing should be returned
```

### **Remediation:**

- **IF** - a separate partition exists for `/dev/shm`.

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.

#### *Example:*

```
tmpfs /dev/shm      tmpfs      defaults,rw,nosuid,nodev,noexec,relatime 0 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. NIST SP 800-53 Rev. 5: AC-3, MP-2

## **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
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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
T1200, T1200.000	TA0005	M1022

### **1.1.2.2.3 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:**

- **IF** - a separate partition exists for `/dev/shm`, verify that the `nosuid` option is set.

```
# findmnt -kn /dev/shm | grep -v 'nosuid'  
Nothing should be returned
```

#### **Remediation:**

- **IF** - a separate partition exists for `/dev/shm`.

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.

#### **Example:**

```
tmpfs /dev/shm      tmpfs      defaults,rw,nosuid,nodev,noexec,relatime  0 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. NIST SP 800-53 Rev. 5: AC-3, MP-2

#### **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
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1548, T1548.001	TA0005	M1038

#### *1.1.2.2.4 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:**

- **IF** - a separate partition exists for `/dev/shm`, verify that the `noexec` option is set.

```
# findmnt -kn /dev/shm | grep -v 'noexec'  
Nothing should be returned
```

##### **Remediation:**

- **IF** - a separate partition exists for `/dev/shm`.  
Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/dev/shm` partition.

##### **Example:**

```
tmpfs /dev/shm      tmpfs      defaults,rw,nosuid,nodev,noexec,relatime  0 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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1204, T1204.002	TA0005	M1022

### 1.1.2.3 Configure /home

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

Finding user home directories can be done by looking in `/etc/passwd`, looking over the mounted file systems with `mount` or querying the relevant database with `getent`.

```
for user in $(awk -F ':' '{print $1}' /etc/passwd); do echo "${user} - $(sudo getent passwd ${user} | awk -F ':' '{print $NF}')"; done
```

### *1.1.2.3.1 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 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.

Configuring `/home` 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. 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.

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 -kn /home  
/home  /dev/sdb  ext4  rw,nosuid,nodev,noexec,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/>
2. NIST SP 800-53 Rev. 5: CM-7

## 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
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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
T1499, T1499.001	TA0005	M1038

### *1.1.2.3.2 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 `/home`.

#### **Audit:**

- **IF** - a separate partition exists for `/home`, verify that the `nodev` option is set.

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

*Example:*

```
# findmnt -kn /home | grep -v nodev
```

```
Nothing should be returned
```

#### **Remediation:**

- **IF** - a separate partition exists for `/home`.

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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1200, T1200.000	TA0005	M1038

### *1.1.2.3.3 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:**

- IF - a separate partition exists for `/home`, verify that the `nosuid` option is set.

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

*Example:*

```
# findmnt -kn /home | grep -v nosuid
```

```
Nothing should be returned
```

#### **Remediation:**

- IF - a separate partition exists for `/home`.

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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1548, T1548.001	TA0005	M1022

#### **1.1.2.4 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.

#### *1.1.2.4.1 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 follows.

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. 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.

Configuring `/var` 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.

An example of exploiting `/var` may be an attacker establishing a hard-link to a system `setuid` program and waiting for it to be updated. Once the program is updated, the hard-link can be broken and the attacker would have their 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 -kn /var  
  
/var  /dev/sdb  ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

## 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/>
2. NIST SP 800-53 Rev. 5: CM-7

## 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
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1499, T1499.001	TA0006	M1022

#### *1.1.2.4.2 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:**

- **IF** - a separate partition exists for `/var`, verify that the `nodev` option is set.

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

*Example:*

```
# findmnt -kn /var | grep -v nodev  
Nothing should be returned
```

##### **Remediation:**

- **IF** - a separate partition exists for `/var`.

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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1200, T1200.000	TA0005	M1022

### *1.1.2.4.3 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:**

- IF - a separate partition exists for `/var`, verify that the `nosuid` option is set.

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

*Example:*

```
# findmnt -kn /var | grep -v nosuid
```

```
Nothing should be returned
```

#### **Remediation:**

- IF - a separate partition exists for `/var`.

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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1548, T1548.001	TA0005	M1022

### **1.1.2.5 Configure /var/tmp**

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

### **1.1.2.5.1 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 files residing in `/var/tmp` are to be preserved between reboots.

#### **Rationale:**

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

Configuring `/var/tmp` 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.

#### **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 -kn /var/tmp
/var/tmp  /dev/sdb ext4    rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **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/>
2. NIST SP 800-53 Rev. 5: CM-7

## 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
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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
T1499, T1499.001	TA0005	M1022

## **1.1.2.5.2 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:**

- IF - a separate partition exists for `/var/tmp`, verify that the `nodev` option is set.  
Run the following command to verify that the `nodev` mount option is set.

*Example:*

```
# findmnt -kn /var/tmp | grep -v nodev  
Nothing should be returned
```

### **Remediation:**

- IF - a separate partition exists for `/var/tmp`.  
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  
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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1499, T1499.001	TA0005	M1022

### **1.1.2.5.3 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:**

- **IF** - a separate partition exists for `/var/tmp`, verify that the `nosuid` option is set.  
Run the following command to verify that the `nosuid` mount option is set.

*Example:*

```
# findmnt -kn /var/tmp | grep -v nosuid  
Nothing should be returned
```

#### **Remediation:**

- **IF** - a separate partition exists for `/var/tmp`.  
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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1548, T1548.001	TA0005	M1022

#### **1.1.2.5.4 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:**

- IF - a separate partition exists for `/var/tmp`, verify that the `noexec` option is set.  
Run the following command to verify that the `noexec` mount option is set.

*Example:*

```
# findmnt -kn /var/tmp | grep -v noexec
```

Nothing should be returned

##### **Remediation:**

- IF - a separate partition exists for `/var/tmp`.  
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
```

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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1204, T1204.002	TA0005	M1022

### **1.1.2.6 Configure /var/log**

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

### *1.1.2.6.1 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 default installation only creates a single `/` partition. Since the `/var/log` directory contains log files which 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.

Configuring `/var/log` 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.

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 -kn /var/log  
/var/log /dev/sdb ext4    rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **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/>
2. NIST SP 800-53 Rev. 5: CM-7

## 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	<b>8.3 Ensure Adequate Audit Log Storage</b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	<b>6.4 Ensure adequate storage for logs</b> 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

## **1.1.2.6.2 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:**

- **IF** - a separate partition exists for `/var/log`, verify that the `nodev` option is set.  
Run the following command to verify that the `nodev` mount option is set.

*Example:*

```
# findmnt -kn /var/log | grep -v nodev
Nothing should be returned
```

### **Remediation:**

- **IF** - a separate partition exists for `/var/log`.  
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
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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1200, T1200.000	TA0005	M1038

### **1.1.2.6.3 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:**

- **IF** - a separate partition exists for `/var/log`, verify that the `nosuid` option is set.  
Run the following command to verify that the `nosuid` mount option is set.

*Example:*

```
# findmnt -kn /var/log | grep -v nosuid  
Nothing should be returned
```

#### **Remediation:**

- **IF** - a separate partition exists for `/var/log`.  
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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1548, T1548.001	TA0005	M1022

#### **1.1.2.6.4 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:**

- IF - a separate partition exists for `/var/log`, verify that the `noexec` option is set.  
Run the following command to verify that the `noexec` mount option is set.

*Example:*

```
# findmnt -kn /var/log | grep -v noexec
```

Nothing should be returned

##### **Remediation:**

- IF - a separate partition exists for `/var/log`.

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
```

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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1204, T1204.002	TA0005	M1022

### **1.1.2.7 Configure /var/log/audit**

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

### **1.1.2.7.1 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 default installation only creates a single `/` partition. Since the `/var/log/audit` directory contains the `audit.log` file which 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.

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.

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 -kn /var/log/audit  
/var/log/audit /dev/sdb ext4    rw,nosuid,nodev,noexec,relatime,seclabel
```

## 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/>
2. NIST SP 800-53 Rev. 5: CM-7

## 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
v8	<b>8.3 Ensure Adequate Audit Log Storage</b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	<b>6.4 Ensure adequate storage for logs</b> 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

## *1.1.2.7.2 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:**

- **IF** - a separate partition exists for `/var/log/audit`, verify that the `nodev` option is set.  
Run the following command to verify that the `nodev` mount option is set.

*Example:*

```
# findmnt -kn /var/log/audit | grep -v nodev
```

```
Nothing should be returned
```

### **Remediation:**

- **IF** - a separate partition exists for `/var/log/audit`.

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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1200, T1200.000	TA0005	M1022

### **1.1.2.7.3 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:**

- IF - a separate partition exists for `/var/log/audit`, verify that the `nosuid` option is set.  
Run the following command to verify that the `nosuid` mount option is set.

#### *Example:*

```
# findmnt -kn /var/log/audit | grep -v nosuid  
Nothing should be returned
```

#### **Remediation:**

- IF - a separate partition exists for `/var/log/audit`.  
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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1548, T1548.001	TA0005	M1022

#### **1.1.2.7.4 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:**

- **IF** - a separate partition exists for `/var/log/audit`, verify that the `noexec` option is set.  
Run the following command to verify that the `noexec` mount option is set.

*Example:*

```
# findmnt -kn /var/log/audit | grep -v noexec
```

```
Nothing should be returned
```

##### **Remediation:**

- **IF** - a separate partition exists for `/var/log/audit`.

Edit the `/etc/fstab` file and add `noexec` 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.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1204, T1204.002	TA0005	M1022

## **1.2 Package Management**

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. Organizations may prefer to test patches against their environment on a non-production system before rolling out to production.

Outdated software is vulnerable to cyber criminals and hackers. Software updates help reduce the risk to your organization. The release of software update notes often reveals the patched exploitable entry points to the public. Public knowledge of these exploits can make your organization more vulnerable to malicious actors attempting to gain entry to your system's data.

Software updates often offer new and improved features and speed enhancements.

For the purpose of this benchmark, the requirement is to ensure that a patch management process is defined and maintained, the specifics of which are left to the organization.

### **1.2.1 Configure Package Repositories**

Outdated software is vulnerable to cyber criminals and hackers. Software updates help reduce the risk to your organization. The release of software update notes often reveals the patched exploitable entry points to the public. Public knowledge of these exploits can make your organization more vulnerable to malicious actors attempting to gain entry to your system's data.

Software updates often offer new and improved features and speed enhancements.

### *1.2.1.1 Ensure GPG keys are configured (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Most package 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.

#### **References:**

1. NIST SP 800-53 Rev. 5: SI-2

## CIS Controls:

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

### *1.2.1.2 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.

#### **References:**

1. NIST SP 800-53 Rev. 5: SI-2

## CIS Controls:

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

## **1.2.2 Configure Package Updates**

### *1.2.2.1 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 update  
# apt -s upgrade
```

#### **Remediation:**

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

```
# apt update  
  
# apt upgrade  
- OR -  
# apt dist-upgrade
```

#### **References:**

1. NIST SP 800-53 Rev. 5: SI-2

## **Additional Information:**

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

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

## **CIS Controls:**

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

**MITRE ATT&CK Mappings:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1195, T1195.001	TA0005	M1051

## 1.3 Mandatory Access Control

Mandatory Access Control (MAC) provides an additional layer of access restrictions to processes on top of the base Discretionary Access Controls. By restricting how processes can access files and resources on a system the potential impact from vulnerabilities in the processes can be reduced.

**Impact:** Mandatory Access Control limits the capabilities of applications and daemons on a system, while this can prevent unauthorized access the configuration of MAC can be complex and difficult to implement correctly preventing legitimate access from occurring.

### **1.3.1 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/>

### *1.3.1.1 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:**

Run the following command to verify that `apparmor` is installed:

```
# dpkg-query -s apparmor &>/dev/null && echo "apparmor is installed"  
apparmor is installed
```

Run the following command to verify that `apparmor-utils` is installed:

```
# dpkg-query -s apparmor-utils &>/dev/null && echo "apparmor-utils is  
installed"  
apparmor-utils is installed
```

#### **Remediation:**

Install AppArmor.

```
# apt install apparmor apparmor-utils
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AC-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	TA0003	M1026

### *1.3.1.2 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
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AC-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	TA0003	M1026

### *1.3.1.3 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*

## **References:**

1. NIST SP 800-53 Rev. 5: AC-3

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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
T1497	TA0005	

### *1.3.1.4 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

#### **References:**

1. NIST SP 800-53 Rev. 5: AC-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	M1048

## **1.4 Configure Bootloader**

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

### *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 to do so, the configuration files will have to be edited via a 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. A 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>
# awk -F. '/^\s*password/ {print $1"."$2"."$3}' /boot/grub/grub.cfg
password_pbkdf2 <username> grub.pbkdf2.sha512
```

## **Remediation:**

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

```
# grub-mkpasswd-pbkdf2 --iteration-count=600000 --salt=64  
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  
exec tail -n +2 $0  
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.

## **References:**

1. NIST SP 800-53 Rev. 5: AC-3

## **Additional Information:**

Changes to `/etc/grub.d/10_linux` may be overwritten during updates to the `grub-common` package. You should review any changes to this file before rebooting otherwise the system may unexpectedly prompt for a password on the next boot.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1542, T1542.000	TA0003	M1046

## *1.4.2 Ensure access to bootloader config is 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 0600 or more restrictive.**

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: ( %g/ %G)'  
/boot/grub/grub.cfg  
  
Access: (0600/-rw-----)  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-x,go-rwx /boot/grub/grub.cfg
```

### **Default Value:**

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3

## **Additional Information:**

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

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

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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
T1542, T1542.000	TA0005, TA0007	M1022

## **1.5 Configure Additional Process Hardening**

## *1.5.1 Ensure address space layout randomization 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 script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `kernel.randomize_va_space` is set to 2

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=(kernel.randomize_va_space=2)
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po '^h*([^\n\r]+|#[^\n\r\h]+\.conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="" read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// /}"; l_fkpvvalue="${l_fkpvvalue// /}"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\"\n"
                fi
            done < <(grep -Po -- "^\h*$l_kpname\h*=\\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n      ** Note:\n\"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS="" read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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 "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

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

- `kernel.randomize_va_space = 2`

### *Example:*

```
# printf "%s\n" "kernel.randomize_va_space = 2" >> /etc/sysctl.d/60-kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

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

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### **Default Value:**

`kernel.randomize_va_space = 2`

### **References:**

1. <http://manpages.ubuntu.com/manpages/focal/man5/sysctl.d.5.html>
2. CCI-000366: The organization implements the security configuration settings
3. NIST SP 800-53 Rev. 5: CM-6

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>10.5 Enable Anti-Exploitation Features</b> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	<b>8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</b> 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.		●	●

**MITRE ATT&CK Mappings:**

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

## *1.5.2 Ensure ptrace\_scope is restricted (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `ptrace()` system call provides a means by which one process (the "tracer") may observe and control the execution of another process (the "tracee"), and examine and change the tracee's memory and registers.

### **Rationale:**

If one application is compromised, it would be possible for an attacker to attach to other running processes (e.g. Bash, Firefox, SSH sessions, GPG agent, etc) to extract additional credentials and continue to expand the scope of their attack.

Enabling restricted mode will limit the ability of a compromised process to `PTRACE_ATTACH` on other processes running under the same user. With restricted mode, `ptrace` will continue to work with root user.

### **Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `kernel.yama.ptrace_scope` is set to 1

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("kernel.yama.ptrace_scope=1")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po '^h*([^\n\r]+|#[^\n\r\h]+\.\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS= read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// /}"; l_fkpvvalue="${l_fkpvvalue// /}"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\"\n"
                fi
            done < <(grep -Po -- "^\h*$l_kpname\h*=\\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n      ** Note:\n\"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS= read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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:**

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

- `kernel.yama.ptrace_scope = 1`

### **Example:**

```
# printf "%s\n" "kernel.yama.ptrace_scope = 1" >> /etc/sysctl.d/60-kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.yama.ptrace_scope=1
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## **References:**

1. <https://www.kernel.org/doc/Documentation/security/Yama.txt>
2. <https://github.com/raj3shp/termspy>
3. NIST SP 800-53 Rev. 5: CM-6

## **Additional Information:**

Ptrace is very rarely used by regular applications and is mostly used by debuggers such as `gdb` and `strace`.

## **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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1055, T1055.008	TA0005	M1040

### *1.5.3 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 command and verify output matches:

```
# grep -Ps -- '^h*\h+hard\h+core\h+0\b' /etc/security/limits.conf  
/etc/security/limits.d/*  
  
* hard core 0
```

Run the following script to verify `fs.suid_dumpable = 0`:

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `fs.suid_dumpable` is set to 0

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("fs.suid_dumpable=0")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po '^h*([^\n\r]+|#[^\n\r\h]+\.\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="" read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// /}"; l_fkpvvalue="${l_fkpvvalue// /}"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\"\n"
                fi
            done < <(grep -Po -- "^\h*$l_kpname\h*=\\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n      ** Note:\n\"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS="" read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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
}

```

Run the following command to check if systemd-coredump is installed:

```
# systemctl list-unit-files | grep coredump
```

if anything 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 file in `/etc/sysctl.d/` ending in `.conf`:

- `fs.suid_dumpable = 0`

### Example:

```
# printf "%s\n" "fs.suid_dumpable = 0" >> /etc/sysctl.d/60-fs_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w fs.suid_dumpable=0
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

-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
```

### References:

1. NIST SP 800-53 Rev. 5: CM-6

### MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0007	M1057

### *1.5.4 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-query -s prelink &>/dev/null && echo "prelink is installed"
```

Nothing should be returned.

#### **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
```

#### **References:**

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.14 Log Sensitive Data Access</b>            Log sensitive data access, including modification and disposal.</p>			●
v7	<p><b>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</b>            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

## *1.5.5 Ensure Automatic Error Reporting is not enabled (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The Apport Error Reporting Service automatically generates crash reports for debugging

### **Rationale:**

Apport collects potentially sensitive data, such as core dumps, stack traces, and log files. They can contain passwords, credit card numbers, serial numbers, and other private material.

### **Audit:**

Run the following command to verify that the Apport Error Reporting Service is not enabled:

```
# dpkg-query -s apport &> /dev/null && grep -Psi --  
'^h*enabled|h*=h*[^0]\b' /etc/default/apport
```

Nothing should be returned

Run the following command to verify that the apport service is not active:

```
# systemctl is-active apport.service | grep '^active'
```

Nothing should be returned

### **Remediation:**

Edit `/etc/default/apport` and add or edit the `enabled` parameter to equal 0:

```
enabled=0
```

Run the following commands to stop and mask the apport service

```
# systemctl stop apport.service  
# systemctl mask apport.service
```

**- OR -**

Run the following command to remove the apport package:

```
# apt purge apport
```

### **Default Value:**

`enabled=1`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></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><b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>	●	●	●

## 1.6 Configure 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.

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/>

The `/etc/motd`, `/etc/issue`, and `/etc/issue.net` files govern warning banners for standard command line logins for both local and remote users.

**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.

## *1.6.1 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 that the contents match site policy:

```
# cat /etc/motd
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\\\v|\\\\r|\\\\m|\\\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's///g'))" /etc/motd
```

## **Remediation:**

Edit the `/etc/motd` file with the appropriate contents according to your site policy, remove any instances of `\m`, `\r`, `\s`, `\v` or references to the OS platform

- OR -

- IF - the `motd` is not used, this file can be removed.

Run the following command to remove the `motd` file:

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

## **References:**

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

## **MITRE ATT&CK Mappings:**

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

## *1.6.2 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

*Example:*

```
# echo "Authorized users only. All activity may be monitored and reported." >
/etc/issue
```

**References:**

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

**MITRE ATT&CK Mappings:**

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

### *1.6.3 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

*Example:*

```
# echo "Authorized users only. All activity may be monitored and reported." >
/etc/issue.net
```

## **References:**

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

## **MITRE ATT&CK Mappings:**

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

## *1.6.4 Ensure access to /etc/motd is 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 access configured, it could be modified by unauthorized users with incorrect or misleading information.

### **Audit:**

Run the following command and verify that if `/etc/motd` exists, Access is 644 or more restrictive, Uid and Gid are both 0/root:

```
# [ -e /etc/motd ] && stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: { %g/ %G)' /etc/motd
Access: (0644/-rw-r--r--)  Uid: ( 0/ root)  Gid: ( 0/ root)
-- OR --
Nothing is returned
```

### **Remediation:**

Run the following commands to set mode, owner, and group 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
```

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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, T1222.002	TA0005	M1022

## *1.6.5 Ensure access to /etc/issue is 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 access configured, it could be modified by unauthorized users with incorrect or misleading information.

### **Audit:**

Run the following command and verify Access is 644 or more restrictive and Uid and Gid are both 0/root:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: { %g/ %G)' /etc/issue
Access: (0644/-rw-r--r--)  Uid: ( 0/ root)  Gid: { 0/ root}
```

### **Remediation:**

Run the following commands to set mode, owner, and group 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)

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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, T1222.002	TA0005	M1022

## *1.6.6 Ensure access to /etc/issue.net is 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 access configured, it could be modified by unauthorized users with incorrect or misleading information.

### **Audit:**

Run the following command and verify Access is 644 or more restrictive and Uid and Gid are both 0/root:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: { %g/ %G)' /etc/issue.net
Access: (0644/-rw-r--r--)  Uid: ( 0/ root)  Gid: ( 0/ root)
```

### **Remediation:**

Run the following commands to set mode, owner, and group 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)

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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, T1222.002	TA0005	M1022

## 1.7 Configure GNOME Display Manager

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

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

### *1.7.1 Ensure GDM 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 -s gdm3 &>/dev/null && echo "gdm3 is installed"
```

Nothing should be returned.

#### **Remediation:**

Run the following commands to uninstall `gdm3` and remove unused dependencies:

```
# apt purge gdm3  
# apt autoremove gdm3
```

#### **References:**

1. NIST SP 800-53 Rev. 5: CM-11

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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
T1543, T1543.002	TA0002	M1033

## *1.7.2 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:**

#### **- IF - GDM is installed:**

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; then
        l_pq="dpkg-query -s"
    elif command -v rpm &> /dev/null; 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 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pk\" exists on
the system\n - checking configuration"
    done
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        echo -e "$l_pkgoutput"
        # Look for existing settings and set variables if they exist
        l_gdmfile=$(grep -Prils '^h*banner-message-enable\b' /etc/dconf/db/*.d)
        if [ -n "$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]}' <<< "$l_gdmfile")
            # Check if banner message is enabled
            if grep -Pisq '^h*banner-message-enable=true\b' "$l_gdmfile"; then
                l_output="$l_output\n - The \"banner-message-enable\" option is enabled in
\"$l_gdmfile\""
            else
                l_output2="$l_output2\n - The \"banner-message-enable\" option is not enabled"
            fi
            l_lsbt=$(grep -Pios '^h*banner-message-text=.*\$' "$l_gdmfile")
            if [ -n "$l_lsbt" ]; then
                l_output="$l_output\n - The \"banner-message-text\" option is set in \"$l_gdmfile\"\n
- banner-message-text is set to:\n - \"$l_lsbt\""
            else
                l_output2="$l_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
                l_output="$l_output\n - The \"$l_gdmprofile\" profile exists"
            else
                l_output2="$l_output2\n - The \"$l_gdmprofile\" profile doesn't exist"
            fi
            if [ -f "/etc/dconf/db/$l_gdmprofile" ]; then
                l_output="$l_output\n - The \"$l_gdmprofile\" profile exists in the dconf database"
            else
                l_output2="$l_output2\n - The \"$l_gdmprofile\" profile doesn't exist in the dconf
database"
            fi
        else
            l_output2="$l_output2\n - The \"banner-message-enable\" option isn't configured"
        fi
    else
        echo -e "\n\n - GNOME Desktop Manager isn't installed\n - Recommendation is Not
Applicable\n- Audit result:\n *** PASS ***\n"
    fi
    # Report results. If no failures output in l_output2, we pass
    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:** banner-message-text may be set in accordance with local site policy

## Remediation:

- IF - GDM is installed:

Run the following script to set and enable the text banner message on the login screen:

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

{
    l_pkgoutput=""
    if command -v dpkg-query &> /dev/null; then
        l_pq="dpkg-query -s"
    elif command -v rpm &> /dev/null; then
        l_pq="rpm -q"
    fi
    l_pc1="gdm gdm3" # Space separated list of packages to check
    for l_pk in $l_pc1; do
        $l_pq "$l_pk" &> /dev/null && 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*/\1true\3//' "$l_kfile"
                #             sed -ri '/^s*\[org/gnome/login-screen\]/ a\\nbanner-message-enable=true'
                "$l_kfile"
            fi
            if ! grep -Piq "^h*banner-message-text=[\'\"]+\S+" "$l_kfile"; then
                sed -ri "/^s*banner-message-enable/ a\\banner-message-text=$l_bmessage" "$l_kfile"
            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
    }
}
```

## Notes:

- 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.

**Default Value:**

disabled

**References:**

1. <https://help.gnome.org/admin/system-admin-guide/stable/login-banner.html.en>
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**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.

**MITRE ATT&CK Mappings:**

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

### *1.7.3 Ensure GDM 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:**

- IF - GDM is installed:

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; then
        l_pq="dpkg-query -s"
    elif command -v rpm &> /dev/null; 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 && 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$output\n"
        else
            echo -e "$l_pkgoutput\n- Audit Result:\n      *** FAIL:
***\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:**

- IF - GDM is installed:

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.

## **Default Value:**

false

## **References:**

1. <https://help.gnome.org/admin/system-admin-guide/stable/login-userlist-disable.html.en>
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**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

## *1.7.4 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.

### **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 commands to verify that the screen locks when the user is idle:

```
# gsettings get org.gnome.desktop.screensaver lock-delay
uint32 5
# gsettings get org.gnome.desktop.session idle-delay
uint32 900
```

### **Notes:**

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

## **Remediation:**

Run the following commands to enable screen locks when the user is idle:

```
# gsettings set org.gnome.desktop.screensaver lock-delay 5  
# gsettings set org.gnome.desktop.session idle-delay 900
```

- OR-

1. Create or edit the user profile 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.

2. Create the directory `/etc/dconf/db/local.d/` if it doesn't already exist:
3. Create the key file `/etc/dconf/db/local.d/00-screensaver` to provide information for the `local` database:

### *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 180  
  
# Specify the dconf path  
[org/gnome/desktop/screensaver]  
  
# Number of seconds after the screen is blank before locking the screen  
lock-delay:uint32 0
```

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

4. Run the following command to update the system databases:

```
# dconf update
```

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

**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>  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>  Automatically lock workstation sessions after a standard period of inactivity.</p>	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1461	TA0027	M1012

## *1.7.5 Ensure GDM screen locks cannot be overridden (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

GNOME Desktop Manager can lock down specific settings by using the lockdown mode in dconf to 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.

### **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 cannot be overridden:

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

{
    # Check if GNOME 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 -s"
    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="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
        done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        # Check if the idle-delay is locked
        if grep -Psrilq '^h*idle-delay|h*=\\h*uint32\\h+d+\\b' /etc/dconf/db/*; then
            if grep -Prilq '\\/org\\/gnome\\/desktop\\/session\\/idle-delay\\b' /etc/dconf/db/*/locks;
        then
            l_output="$l_output\n - \"idle-delay\" is locked"
            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 cannot be locked"
        fi
        # Check if the lock-delay is locked
        if grep -Psrilq '^h*lock-delay|h*=\\h*uint32\\h+d+\\b' /etc/dconf/db/*; then
            if grep -Prilq '\\/org\\/gnome\\/desktop\\/screensaver\\/lock-delay\\b' /etc/dconf/db/*/locks;
        then
            l_output="$l_output\n - \"lock-delay\" is locked"
            else
            l_output2="$l_output2\n - \"lock-delay\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"lock-delay\" is not set so it cannot be locked"
        fi
    else
        l_output="$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:$l_output\n"
    fi
}
```

## **Remediation:**

1. To prevent the user from overriding these settings, create the file `/etc/dconf/db/local.d/locks/screensaver` with the following content:

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

2. 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>
3. NIST SP 800-53 Rev. 5: CM-11

## **CIS Controls:**

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

## **MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1456	TA0027	M1001

## *1.7.6 Ensure GDM 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 - GDM is installed:

Run the following script to verify automatic mounting is disabled:

```

#!/usr/bin/env bash

{
    l_pkgoutput="" l_output="" l_output2=""
    # Check if GNOME Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -s"
    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="$l_pkgoutput\n -\n Package: \"$l_pn\" exists on the system\n - checking configuration"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        echo -e "$l_pkgoutput"
        # Look for existing settings and set variables if they exist
        l_kfile=$(grep -Prils -- '^h*automount\b' /etc/dconf/db/*.d)
        l_kfile2=$(grep -Prils -- '^h*automount-open\b' /etc/dconf/db/*.d)
        # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
        if [ -f "$l_kfile" ]; then
            l_gpname=$(awk -F'\/' '{split(${NF-1}),a,".");print a[1]}' <<<
"$l_kfile")
        elif [ -f "$l_kfile2" ]; then
            l_gpname=$(awk -F'\/' '{split(${NF-1}),a,".");print a[1]}' <<<
"$l_kfile2")
        fi
        # If the profile name exist, continue checks
        if [ -n "$l_gpname" ]; then
            l_gpdir="/etc/dconf/db/$l_gpname.d"
            # Check if profile file exists
            if grep -Pq -- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*;
        then
            l_output="$l_output\n - dconf database profile file \"$(grep -Pl
-- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*)\\" exists"
            else
                l_output2="$l_output2\n - dconf database profile isn't set"
            fi
            # Check if the dconf database file exists
            if [ -f "/etc/dconf/db/$l_gpname" ]; then
                l_output="$l_output\n - The dconf database \"$l_gpname\" exists"
            else
                l_output2="$l_output2\n - The dconf database \"$l_gpname\""
            doesn't exist"
            fi
            # check if the dconf database directory exists
            if [ -d "$l_gpdir" ]; then
                l_output="$l_output\n - The dconf directory \"$l_gpdir\" exitst"
            else
                l_output2="$l_output2\n - The dconf directory \"$l_gpdir\""
            doesn't exist"
            fi
        else
            l_output2="$l_output2\n - The dconf database \"$l_gpname\""
        done
    fi
}

```

```

# check automount setting
if grep -Pqrs -- '^h*automount\h*=\\h*false\b' "$l_kfile"; then
    l_output="$l_output\n - \"automount\" is set to false in:
\"$l_kfile\""
else
    l_output2="$l_output2\n - \"automount\" is not set correctly"
fi
# check automount-open setting
if grep -Pqs -- '^h*automount-open\h*=\\h*false\b' "$l_kfile2"; then
    l_output="$l_output\n - \"automount-open\" is set to false in:
\"$l_kfile2\""
else
    l_output2="$l_output2\n - \"automount-open\" is not set
correctly"
fi
else
    # Setings don't exist. Nothing further to check
    l_output2="$l_output2\n - neither \"automount\" or \"automount-
open\" is set"
fi
else
    l_output="$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
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:**

### **- IF - GDM is installed:**

Run the following script to disable automatic mounting of media for all GNOME users:

```

#!/usr/bin/env bash

{
    l_pkgoutput=""
    l_gpname="local" # Set to desired dconf profile name (default is local)
    # Check if GNOME Desktop Manager is installed. If package isn't
installed, recommendation is Not Applicable\n
    # determine system's package manager
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -s"
    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_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
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        echo -e "$l_pkgoutput"
        # Look for existing settings and set variables if they exist
        l_kfile=$(grep -Prils -- '^h*automount\b' /etc/dconf/db/*.d)
        l_kfile2=$(grep -Prils -- '^h*automount-open\b' /etc/dconf/db/*.d)
        # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
        if [ -f "$l_kfile" ]; then
            l_gpname=$(awk -F'/' '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile")
            echo " - updating dconf profile name to \"$l_gpname\""
        elif [ -f "$l_kfile2" ]; then
            l_gpname=$(awk -F'/' '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile2")
            echo " - updating dconf profile name to \"$l_gpname\""
        fi
        # check for consistency (Clean up configuration if needed)
        if [ -f "$l_kfile" ] && [ "$(awk -F'/' '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile")" != "$l_gpname" ]; then
            sed -ri "/^s*automount\s*/s/^/# /" "$l_kfile"
            l_kfile="/etc/dconf/db/$l_gpname.d/00-media-automount"
        fi
        if [ -f "$l_kfile2" ] && [ "$(awk -F'/' '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile2")" != "$l_gpname" ]; then
            sed -ri "/^s*automount-open\s*/s/^/# /" "$l_kfile2"
        fi
        [ -z "$l_kfile" ] && l_kfile="/etc/dconf/db/$l_gpname.d/00-media-automount"
        # Check if profile file exists
        if grep -Pq -- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*; then
            echo -e "\n - dconf database profile exists in: \"$(grep -Pl --
"^\h*system-db:$l_gpname\b" /etc/dconf/profile/*)\""
        else
            if [ ! -f "/etc/dconf/profile/user" ]; then
                l_gpfile="/etc/dconf/profile/user"
            else
                l_gpfile="/etc/dconf/profile/user2"
            fi
        fi
    done
}

```

```

        echo -e " - creating dconf database profile"
    {
        echo -e "\nuser-db:user"
        echo "system-db:$l_gpname"
    } >> "$l_gpfile"
fi
# create dconf directory if it doesn't exists
l_gpdir="/etc/dconf/db/$l_gpname.d"
if [ -d "$l_gpdir" ]; then
    echo " - The dconf database directory \"$l_gpdir\" exists"
else
    echo " - creating dconf database directory \"$l_gpdir\""
    mkdir "$l_gpdir"
fi
# check automount-open setting
if grep -Pqs -- '^h*automount-open|h*=h*false\b' "$l_kfile"; then
    echo " - \"automount-open\" is set to false in: \"$l_kfile\""
else
    echo " - creating \"automount-open\" entry in \"$l_kfile\""
    ! grep -Psq -- '\^h*[org/gnome/desktop/media-handling]\b' "$l_kfile" && echo '[org/gnome/desktop/media-handling]' >> "$l_kfile"
    sed -ri '/^\s*[org/gnome/desktop/media-handling]\b/a\nautomount-open=false' "$l_kfile"
    fi
# check automount setting
if grep -Pqs -- '^h*automount|h*=h*false\b' "$l_kfile"; then
    echo " - \"automount\" is set to false in: \"$l_kfile\""
else
    echo " - creating \"automount\" entry in \"$l_kfile\""
    ! grep -Psq -- '\^h*[org/gnome/desktop/media-handling]\b' "$l_kfile" && echo '[org/gnome/desktop/media-handling]' >> "$l_kfile"
    sed -ri '/^\s*[org/gnome/desktop/media-handling]\b/a\nautomount=false' "$l_kfile"
    fi
# update dconf database
dconf update
else
    echo -e "\n - GNOME Desktop Manager package is not installed on the
system\n - Recommendation is not applicable"
    fi
}

```

## References:

1. <https://access.redhat.com/solutions/20107>
2. 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>10.3 <u>Disable Autorun and Autoplay for Removable Media</u>            Disable autorun and autoplay auto-execute functionality for removable media.</p>	●	●	●
v7	<p>8.5 <u>Configure Devices Not To Auto-run Content</u>            Configure devices to not auto-run content from removable media.</p>	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1091, T1091.000	TA0008	M1042

## *1.7.7 Ensure GDM disabling automatic mounting of removable media is not overridden (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.

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.

### **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

### **Audit:**

Run the following script to verify automatic mounting of removable media is not overridden and correctly configured in a configuration file:

- automount=false
- automount-open=false

```

#!/usr/bin/env bash

{
    # Check if GNOME Desktop Manager is installed.
    l_pkgoutput=""
    if command -v dpkg-query &> /dev/null; then
        l_pq="dpkg-query -s"
    elif command -v rpm &> /dev/null; 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 && l_pkgoutput="$l_pkgoutput\n - Package:
\"$l_pn\" exists on the system\n - Checking configuration"
    done
    # Check for GDM configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        l_output=""
        l_output2=""
        # Search /etc/dconf/db/local.d/ for automount settings
        l_automount_setting=$(grep -Psir -- '^h*automount=false\b' /etc/dconf/db/local.d/*)
        l_automount_open_setting=$(grep -Psir -- '^h*automount-open=false\b' /etc/dconf/db/local.d/*)
        # Check for automount setting
        if [[ -n "$l_automount_setting" ]]; then
            l_output="$l_output\n - \"automount\" setting found"
        else
            l_output2="$l_output2\n - \"automount\" setting not found"
        fi
        # Check for automount-open setting
        if [[ -n "$l_automount_open_setting" ]]; then
            l_output="$l_output\n - \"automount-open\" setting found"
        else
            l_output2="$l_output2\n - \"automount-open\" setting not found"
        fi
    else
        l_output="$l_output\n - GNOME Desktop Manager package is not installed
on the system\n - Recommendation is not applicable"
    fi
    # Report results. If no failures 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:**

1. To prevent the user from overriding these settings, create the file /etc/dconf/db/local.d/locks/00-media-automount with the following content:

```
[org/gnome/desktop/media-handling]
automount=false
automount-open=false
```

2. Update the systems databases:

```
# dconf update
```

## **References:**

1. <https://help.gnome.org/admin/system-admin-guide/stable/dconf-lockdown.html.en>
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5
3. <https://manpages.ubuntu.com/manpages/trusty/man1/gsettings.1.html>
4. <https://access.redhat.com/solutions/20107>

## **MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1091, T1091.000	TA0001, TA0008	M1042

## *1.7.8 Ensure GDM autorun-never is enabled (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `autorun-never` setting allows the GNOME Desktop Display Manager to disable autorun through GDM.

### **Rationale:**

Malware on removable media may take advantage of Autorun features when the media is inserted into a system and execute.

### **Audit:**

- IF - GDM is installed:

Run the following script to verify that `autorun-never` is set to `true` for GDM:

```

#!/usr/bin/env bash

{
    l_pkgoutput="" l_output="" l_output2=""
    # Check if GNOME Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    if command -v dpkg-query &> /dev/null; then
        l_pq="dpkg-query -s"
    elif command -v rpm &> /dev/null; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pk in $l_pcl; do
        $l_pq "$l_pk" &> /dev/null && l_pkgoutput="$l_pkgoutput\n - Package:
\"$l_pk\" exists on the system\n - checking configuration"
        echo -e "$l_pkgoutput"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        echo -e "$l_pkgoutput"
        # Look for existing settings and set variables if they exist
        l_kfile=$(grep -Prils -- '^h*autorun-never\b' /etc/dconf/db/*.d)
        # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
        if [ -f "$l_kfile" ]; then
            l_gpname=$(awk -F'/' '{split($NF-1),a,".");print a[1]}' <<<
"$l_kfile")
            fi
        # If the profile name exist, continue checks
        if [ -n "$l_gpname" ]; then
            l_gpdir="/etc/dconf/db/$l_gpname.d"
            # Check if profile file exists
            if grep -Pq -- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*;
        then
            l_output="$l_output\n - dconf database profile file \"$(grep -Pl
-- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*)\\" exists"
            else
                l_output2="$l_output2\n - dconf database profile isn't set"
            fi
            # Check if the dconf database file exists
            if [ -f "/etc/dconf/db/$l_gpname" ]; then
                l_output="$l_output\n - The dconf database \"$l_gpname\" exists"
            else
                l_output2="$l_output2\n - The dconf database \"$l_gpname\""
            doesn't exist"
            fi
            # check if the dconf database directory exists
            if [ -d "$l_gpdir" ]; then
                l_output="$l_output\n - The dconf directory \"$l_gpdir\" exitst"
            else
                l_output2="$l_output2\n - The dconf directory \"$l_gpdir\""
            doesn't exist"
            fi
            # check autorun-never setting
            if grep -Pqrs -- '^h*autorun-never\h*=\h*true\b' "$l_kfile"; then
                l_output="$l_output\n - \"autorun-never\" is set to true in:

```

```

\"$1_kfile\"
    else
        l_output2="$1_output2\n - \"autorun-never\" is not set correctly"
    fi
else
    # Settings don't exist. Nothing further to check
    l_output2="$1_output2\n - \"autorun-never\" is not set"
fi
else
    l_output="$1_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
if [ -z "$1_output2" ]; then
    echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
else
    echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
    [ -n "$1_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
fi
}

```

## **Remediation:**

**- IF - GDM is installed:**

Run the following script to set autorun-never to true for GDM users:

```

#!/usr/bin/env bash

{
    l_pkgoutput="" l_output="" l_output2=""
    l_gpname="local" # Set to desired dconf profile name (default is local)
    # Check if GNOME Desktop Manager is installed. If package isn't
installed, recommendation is Not Applicable\n
    # determine system's package manager
    if command -v dpkg-query &> /dev/null; then
        l_pq="dpkg-query -s"
    elif command -v rpm &> /dev/null; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pk in $l_pcl; do
        $l_pq "$l_pk" &> /dev/null && l_pkgoutput="$l_pkgoutput\n - Package:
\"$l_pk\" exists on the system\n - checking configuration"
    done
    echo -e "$l_pkgoutput"
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        echo -e "$l_pkgoutput"
        # Look for existing settings and set variables if they exist
        l_kfile=$(grep -Prils -- '^h*autorun-never\b' /etc/dconf/db/*.{d})
        # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
        if [ -f "$l_kfile" ]; then
            l_gpname=$(awk -F'/' '{split(${NF-1}),a,".");print a[1]}' <<<
"$l_kfile")
            echo " - updating dconf profile name to \"$l_gpname\""
        fi
        [ ! -f "$l_kfile" ] && l_kfile="/etc/dconf/db/$l_gpname.d/00-media-
autorun"
        # Check if profile file exists
        if grep -Pq -- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*; then
            echo -e "\n - dconf database profile exists in: \"$(grep -Pl --
"^\h*system-db:$l_gpname\b" /etc/dconf/profile/*)\""
        else
            [ ! -f "/etc/dconf/profile/user" ] &&
l_gpfile="/etc/dconf/profile/user" || l_gpfile="/etc/dconf/profile/user2"
            echo -e " - creating dconf database profile"
            {
                echo -e "\nuser-db:user"
                echo "system-db:$l_gpname"
            } >> "$l_gpfile"
        fi
        # create dconf directory if it doesn't exists
        l_gpdir="/etc/dconf/db/$l_gpname.d"
        if [ -d "$l_gpdir" ]; then
            echo " - The dconf database directory \"$l_gpdir\" exists"
        else
            echo " - creating dconf database directory \"$l_gpdir\""
            mkdir "$l_gpdir"
        fi
        # check autorun-never setting
        if grep -Pqs -- '^h*autorun-never\b.*=h*true\b' "$l_kfile"; then
            echo " - \"autorun-never\" is set to true in: \"$l_kfile\""
        fi
    done
}

```

```

        else
            echo " - creating or updating \"autorun-never\" entry in
\"$l_kfile\""
            if grep -Psq -- '^h*autorun-never' "$l_kfile"; then
                sed -ri 's/(^s*autorun-never\s*)(\S+)(\s*.*)$/\1true \3/'
"$l_kfile"
            else
                ! grep -Psq -- '\^h*[org/gnome/desktop/media-handling]\b'
"$l_kfile" && echo '[org/gnome/desktop/media-handling]' >> "$l_kfile"
                sed -ri '/^s*[org/gnome/desktop/media-handling]/a
\\nautorun-never=true' "$l_kfile"
            fi
        fi
    else
        echo -e "\n - GNOME Desktop Manager package is not installed on the
system\n - Recommendation is not applicable"
    fi
# update dconf database
dconf update
}

```

### **Default Value:**

false

### **References:**

1. 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	<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.	●	●	●

### **MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1091, T1091.000	TA0001, TA0008	M1042

## *1.7.9 Ensure GDM autorun-never is not overridden (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The autorun-never setting allows the GNOME Desktop Display Manager to disable autorun through GDM.

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.

### **Rationale:**

Malware on removable media may take advantage of Autorun features when the media is inserted into a system and execute.

## Audit:

Run the following script to verify that autorun-never=true cannot be overridden:

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

{
    # Check if GNOME 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; then
        l_pq="dpkg-query -s"
    elif command -v rpm &> /dev/null; 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 && l_pkgoutput="$l_pkgoutput\n - Package:
\"$l_pn\" exists on the system\n - checking configuration"
        done
    # Search /etc/dconf/db/ for [org/gnome/desktop/media-handling] settings)
    l_desktop_media_handling=$(grep -Psir -- '^h*[org/gnome/desktop/media-
handling]' /etc/dconf/db/*)
    if [[ -n "$l_desktop_media_handling" ]]; then
        l_output="" l_output2=""
        l_autorun_setting=$(grep -Psir -- '^h*autorun-never=true\b'
/etc/dconf/db/local.d/*)
        # Check for auto-run setting
        if [[ -n "$l_autorun_setting" ]]; then
            l_output="$l_output\n - \"autorun-never\" setting found"
        else
            l_output2="$l_output2\n - \"autorun-never\" setting not found"
        fi
    else
        l_output="$l_output\n - [org/gnome/desktop/media-handling] setting
not found in /etc/dconf/db/*"
    fi
    # Report results. If no failures output in l_output2, we pass
    [ -n "$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:**

1. To prevent the user from overriding these settings, create the file /etc/dconf/db/local.d/locks/00-media-autorun with the following content:

```
[org/gnome/desktop/media-handling]
autorun-never=true
```

2. Update the systems databases:

```
# dconf update
```

## **References:**

1. 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	<a href="#">10.3 Disable Autorun and Autoplay for Removable Media</a> Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	<a href="#">8.5 Configure Devices Not To Auto-run Content</a> Configure devices to not auto-run content from removable media.	●	●	●

## **MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1091, T1091.000	TA0001, TA0008	M1028

### *1.7.10 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 script and verify the output:

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

{
    while IFS= read -r l_file; do
        awk '/\[xdmcp\]/{f = 1;next } /\[/{ f = 0 } f {if
(/^\s*Enable\s*=\s*true/) print "The file: \"'"$l_file"'\" includes: \"'"$0
"\\" in the \"'[xdmcp]'\" block"}' "$l_file"
        done < <(grep -Psil -- '^h*\[xdmcp\]' /etc/{gdm3,gdm}/custom.conf)
    }
}
```

Nothing should be returned

## **Remediation:**

Edit all files returned by the audit and remove or comment out the `Enable=true` line in the `[xdmcp]` block:

*Example file:*

```
# GDM configuration storage
#
# See /usr/share/gdm/gdm.schemas for a list of available options.

[daemon]
# Uncomment the line below to force the login screen to use Xorg
#WaylandEnable=false

# Enabling automatic login
# AutomaticLoginEnable = true
# AutomaticLogin = user1

# Enabling timed login
# TimedLoginEnable = true
# TimedLogin = user1
# TimedLoginDelay = 10

[security]

[xdmcp]
# Enable=true <- **This line should be removed or commented out**

[chooser]

[debug]
# Uncomment the line below to turn on debugging
# More verbose logs
# Additionally lets the X server dump core if it crashes
#Enable=true
```

## **Default Value:**

false (This is denoted by no Enabled= entry in the [xdmcp] block)

## **References:**

1. NIST SP 800-53 Rev. 5: SI-4

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

## **2 Services**

While applying system updates and patches helps correct known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to disable all services that are not required for normal system operation. This prevents the exploitation of vulnerabilities discovered at a later date. If a service is not enabled, it cannot be exploited. The actions in this section of the document provide guidance on some services which can be safely disabled and under which circumstances, greatly reducing the number of possible threats to the resulting system. Additionally, some services which should remain enabled but with secure configuration are covered as well as insecure service clients.

## 2.1 Configure Server 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 the package be removed.

- IF - the package is required for a dependency:

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy
- Stop and mask the service and/or socket to reduce the potential attack surface

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

```
# systemctl stop <service_name>.socket <service_name>.service  
# systemctl mask <service_name>.socket <service_name>.service
```

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

## *2.1.1 Ensure autofs services are not in use (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 the filesystem 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.

There may be packages that are dependent on the `autofs` package. If the `autofs` package is removed, these dependent packages will be removed as well. Before removing the `autofs` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `autofs.service` leaving the `autofs` package installed.

## 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:

```
# dpkg-query -s autofs &>/dev/null && echo "autofs is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

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

```
# systemctl is-enabled autofs.service 2>/dev/null | grep 'enabled'
```

```
Nothing should be returned
```

Run the following command to verify the `autofs.service` is not active:

```
# systemctl is-active autofs.service 2>/dev/null | grep '^active'
```

```
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `autofs.service` and remove the `autofs` package:

```
# systemctl stop autofs.service  
# apt purge autofs
```

- OR -

- IF - the `autofs` package is required as a dependency:

Run the following commands to stop and mask `autofs.service`:

```
# systemctl stop autofs.service  
# systemctl mask autofs.service
```

## References:

1. NIST SP 800-53 Rev. 5: SI-3, MP-7

## Additional Information:

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

## CIS Controls:

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

## MITRE ATT&CK Mappings:

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

## *2.1.2 Ensure avahi daemon services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 2 - 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.

### **Impact:**

There may be packages that are dependent on the `avahi` package. If the `avahi` package is removed, these dependent packages will be removed as well. Before removing the `avahi` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `avahi-daemon.socket` and `avahi-daemon.service` leaving the `avahi` package installed.

## Audit:

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

```
# dpkg-query -s avahi-daemon &>/dev/null && echo "avahi-daemon is installed"
```

Nothing should be returned.

- OR -

- IF - the `avahi` package is required as a dependency:

Run the following command to verify `avahi-daemon.socket` and `avahi-daemon.service` are not enabled:

```
# systemctl is-enabled avahi-daemon.socket avahi-daemon.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify `avahi-daemon.socket` and `avahi-daemon.service` are not active:

```
# systemctl is-active avahi-daemon.socket avahi-daemon.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `avahi-daemon.socket` and `avahi-daemon.service`, and remove the `avahi-daemon` package:

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

- OR -

- IF - the `avahi-daemon` package is required as a dependency:

Run the following commands to stop and mask the `avahi-daemon.socket` and `avahi-daemon.service`:

```
# systemctl stop avahi-daemon.socket avahi-daemon.service  
# systemctl mask avahi-daemon.socket avahi-daemon.service
```

## References:

1. NIST SP 800-53 Rev. 5: SI-4

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

## *2.1.3 Ensure dhcp server services are not in use (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. There are two versions of the DHCP protocol `DHCPv4` and `DHCPv6`. At startup the server may be started for one or the other via the `-4` or `-6` arguments.

### **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.

### **Impact:**

There may be packages that are dependent on the `isc-dhcp-server` package. If the `isc-dhcp-server` package is removed, these dependent packages will be removed as well. Before removing the `isc-dhcp-server` package, review any dependent packages to determine if they are required on the system.

**- IF -** a dependent package is required: stop and mask the `isc-dhcp-server.service` and `isc-dhcp-server6.service` leaving the `isc-dhcp-server` package installed.

## Audit:

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

```
# dpkg-query -s isc-dhcp-server &>/dev/null && echo "isc-dhcp-server is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify `isc-dhcp-server.service` and `isc-dhcp-server6.service` are not enabled:

```
# systemctl is-enabled isc-dhcp-server.service isc-dhcp-server6.service  
2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify `isc-dhcp-server.service` and `isc-dhcp-server6.service` are not active:

```
# systemctl is-active isc-dhcp-server.service isc-dhcp-server6.service  
2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `isc-dhcp-server.service` and `isc-dhcp-server6.service` and remove the `isc-dhcp-server` package:

```
# systemctl stop isc-dhcp-server.service isc-dhcp-server6.service  
# apt purge isc-dhcp-server
```

- OR -

- IF - the `isc-dhcp-server` package is required as a dependency:

Run the following commands to stop and mask `isc-dhcp-server.service` and `isc-dhcp-server6.service`:

```
# systemctl stop isc-dhcp-server.service isc-dhcp-server6.service  
# systemctl mask isc-dhcp-server isc-dhcp-server6.service
```

## References:

1. More detailed documentation on DHCP is available at <http://www.isc.org/software/dhcp>.
2. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

## 2.1.4 Ensure dns server services are not in use (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.

### Impact:

There may be packages that are dependent on the `bind9` package. If the `bind9` package is removed, these dependent packages will be removed as well. Before removing the `bind9` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `bind9.service` leaving the `bind9` package installed.

### Audit:

Run the following command to verify `bind9` is not installed:

```
# dpkg-query -s bind9 &>/dev/null && echo "bind9 is installed"
```

Nothing should be returned.

- **OR** -

- **IF** - the package is required for dependencies:

Run the following command to verify `bind9.service` is not enabled:

```
# systemctl is-enabled bind9.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify the `bind9.service` is not active:

```
# systemctl is-active bind9.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `bind9.service` and remove the `bind9` package:

```
# systemctl stop bind9.service  
# apt purge bind9
```

- OR -

- IF - the `bind9` package is required as a dependency:

Run the following commands to stop and mask `bind9.service`:

```
# systemctl stop bind9.service  
# systemctl mask bind9.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## 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
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

## *2.1.5 Ensure dnsmasq services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

`dnsmasq` is a lightweight tool that provides DNS caching, DNS forwarding and DHCP (Dynamic Host Configuration Protocol) services.

### **Rationale:**

Unless a system is specifically designated to act as a DNS caching, DNS forwarding and/or DHCP server, it is recommended that the package be removed to reduce the potential attack surface.

### **Impact:**

There may be packages that are dependent on the `dnsmasq` package. If the `dnsmasq` package is removed, these dependent packages will be removed as well. Before removing the `dnsmasq` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `dnsmasq.service` leaving the `dnsmasq` package installed.

## Audit:

Run one of the following commands to verify `dnsmasq` is not installed:

```
# dpkg-query -s dnsmasq &>/dev/null && echo "dnsmasq is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify `dnsmasq.service` is not enabled:

```
# systemctl is-enabled dnsmasq.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify the `dnsmasq.service` is not active:

```
# systemctl is-active dnsmasq.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `dnsmasq.service` and remove `dnsmasq` package:

```
# systemctl stop dnsmasq.service  
# apt purge dnsmasq
```

- OR -

- IF - the `dnsmasq` package is required as a dependency:

Run the following commands to stop and mask the `dnsmasq.service`:

```
# systemctl stop dnsmasq.service  
# systemctl mask dnsmasq.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b></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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b></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

## *2.1.6 Ensure ftp server services are not in use (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.

### **Impact:**

There may be packages that are dependent on the `vsftpd` package. If the `vsftpd` package is removed, these dependent packages will be removed as well. Before removing the `vsftpd` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `vsftpd.service` leaving the `vsftpd` package installed.

## Audit:

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

```
# dpkg-query -s vsftpd &>/dev/null && echo "vsftpd is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify `vsftpd` service is not enabled:

```
# systemctl is-enabled vsftpd.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify the `vsftpd` service is not active:

```
# systemctl is-active vsftpd.service 2>/dev/null | grep '^active'
```

Nothing should be returned

## Note:

- Other ftp server packages may exist. They should also be audited, if not required and authorized by local site policy
- If the package is required for a dependency:
  - Ensure the dependent package is approved by local site policy
  - Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `vsftpd.service` and remove the `vsftpd` package:

```
# systemctl stop vsftpd.service  
# apt purge vsftpd
```

- OR -

- IF - the `vsftpd` package is required as a dependency:

Run the following commands to stop and mask the `vsftpd.service`:

```
# systemctl stop vsftpd.service  
# systemctl mask vsftpd.service
```

**Note:** Other ftp server packages may exist. If not required and authorized by local site policy, they should also be removed. If the package is required for a dependency, the service should be stopped and masked.

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## **Additional Information:**

Additional FTP servers also exist and should be audited.

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> 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

## *2.1.7 Ensure Idap server services are not in use (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.

### **Impact:**

There may be packages that are dependent on the `slapd` package. If the `slapd` package is removed, these dependent packages will be removed as well. Before removing the `slapd` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `slapd.service` leaving the `slapd` package installed.

## Audit:

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

```
# dpkg-query -s slapd >/dev/null && echo "slapd is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify `slapd.service` is not enabled:

```
# systemctl is-enabled slapd.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify `slapd.service` is not active:

```
# systemctl is-active slapd.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `slapd.service` and remove the `slapd` package:

```
# systemctl stop slapd.service  
# apt purge slapd
```

- OR -

- IF - the `slapd` package is required as a dependency:

Run the following commands to stop and mask `slapd.service`:

```
# systemctl stop slapd.service  
# systemctl mask slapd.service
```

## References:

1. For more detailed documentation on OpenLDAP, go to the project homepage at <http://www.openldap.org>.
2. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b></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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b></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

## *2.1.8 Ensure message access server services are not in use (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.

**Note:** Several IMAP/POP3 servers exist and can use other service names. These should also be audited and the packages removed if not required.

### **Impact:**

There may be packages that are dependent on `dovecot-imapd` and/or `dovecot-pop3d` packages. If `dovecot-imapd` and `dovecot-pop3d` packages are removed, these dependent packages will be removed as well. Before removing `dovecot-imapd` and/or `dovecot-pop3d` packages, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask `dovecot.socket` and `dovecot.service` leaving `dovecot-imapd` and/or `dovecot-pop3d` packages installed.

## Audit:

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

```
# dpkg-query -s dovecot-imapd &>/dev/null && echo "dovecot-imapd is installed"
```

Nothing should be returned.

```
# dpkg-query -s dovecot-pop3d &>/dev/null && echo "dovecot-pop3d is installed"
```

Nothing should be returned.

- OR -

- IF - a package is installed **and** is required for dependencies:

Run the following commands to verify `dovecot.socket` and `dovecot.service` are not enabled:

```
# systemctl is-enabled dovecot.socket dovecot.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify `dovecot.socket` and `dovecot.service` are not active:

```
# systemctl is-active dovecot.socket dovecot.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## **Remediation:**

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

Run the following commands to stop dovecot.socket and dovecot.service, and remove the dovecot-imapd and dovecot-pop3d packages:

```
# systemctl stop dovecot.socket dovecot.service  
# apt purge dovecot-imapd dovecot-pop3d
```

**- OR -**

**- IF -** a package is installed **and** is required for dependencies:

Run the following commands to stop and mask dovecot.socket and dovecot.service:

```
# systemctl stop dovecot.socket dovecot.service  
# systemctl mask dovecot.socket dovecot.service
```

## **References:**

1. NIST SP 800-53 Rev. 5: CM-7

## **Additional Information:**

Several IMAP/POP3 servers exist and can use other service names. courier-imap and cyrus-imap are example services that provide a mail server. These and other services should also be audited.

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> 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:**

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

## *2.1.9 Ensure network file system services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network.

### **Rationale:**

If the system does not export NFS shares, it is recommended that the `nfs-kernel-server` package be removed to reduce the remote attack surface.

### **Impact:**

There may be packages that are dependent on the `nfs-kernel-server` package. If the `nfs-kernel-server` package is removed, these dependent packages will be removed as well. Before removing the `nfs-kernel-server` package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the `nfs-server.service` leaving the `nfs-kernel-server` package installed.

## Audit:

Run the following command to verify `nfs-kernel-server` is not installed:

```
# dpkg-query -s nfs-kernel-server &>/dev/null && echo "nfs-kernel-server is installed"
```

Nothing should be returned.

- OR -

- IF - package is required for dependencies:

Run the following command to verify that the `nfs-server.service` is not enabled:

```
# systemctl is-enabled nfs-server.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify the `nfs-server.service` is not active:

```
# systemctl is-active nfs-server.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following command to stop `nfs-server.service` and remove `nfs-kernel-server` package:

```
# systemctl stop nfs-server.service
# apt purge nfs-kernel-server
```

- OR -

- IF - the `nfs-kernel-server` package is required as a dependency:

Run the following commands to stop and mask the `nfs-server.service`:

```
# systemctl stop nfs-server.service
# systemctl mask nfs-server.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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, T1210, T1210.000	TA0008	M1042

## *2.1.10 Ensure nis server services are not in use (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. The NIS client (`ypbind`) was used to bind a machine to an NIS server and receive the distributed configuration files.

### **Rationale:**

`ypserv.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 `ypserv.service` be removed and other, more secure services be used

### **Impact:**

There may be packages that are dependent on the `ypserv` package. If the `ypserv` package is removed, these dependent packages will be removed as well. Before removing the `ypserv` package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the `ypserv.service` leaving the `ypserv` package installed.

## Audit:

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

```
# dpkg-query -s ypserv &>/dev/null && echo "ypserv is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify `ypserv.service` is not enabled:

```
# systemctl is-enabled ypserv.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify `ypserv.service` is not active:

```
# systemctl is-active ypserv.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `ypserv.service` and remove `ypserv` package:

```
# systemctl stop ypserv.service  
# apt purge ypserv
```

- OR -

- IF - the `ypserv` package is required as a dependency:

Run the following commands to stop and mask `ypserv.service`:

```
# systemctl stop ypserv.service  
# systemctl mask ypserv.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

## *2.1.11 Ensure print server services are not in use (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 the `cups` package, or disabling `cups.socket` and/or `cups.service` will prevent printing from the system, a common task for workstation systems.

There may be packages that are dependent on the `cups` package. If the `cups` package is removed, these dependent packages will be removed as well. Before removing the `cups` package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask `cups.socket` and `cups.service` leaving the `cups` package installed.

## Audit:

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

```
# dpkg-query -s cups &>/dev/null && echo "cups is installed"
```

Nothing should be returned.

- OR -

- IF - the `cups` package is required as a dependency:

Run the following command to verify the `cups.socket` and `cups.service` are not enabled:

```
# systemctl is-enabled cups.socket cups.service 2>/dev/null | grep 'enabled'
```

```
Nothing should be returned
```

Run the following command to verify the `cups.socket` and `cups.service` are not active:

```
# systemctl is-active cups.socket cups.service 2>/dev/null | grep '^active'
```

```
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `cups.socket` and `cups.service`, and remove the `cups` package:

```
# systemctl stop cups.socket cups.service  
# apt purge cups
```

- OR -

- IF - the `cups` package is required as a dependency:

Run the following commands to stop and mask the `cups.socket` and `cups.service`:

```
# systemctl stop cups.socket cups.service  
# systemctl mask cups.socket cups.service
```

## References:

1. <http://www.cups.org>
2. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

## *2.1.12 Ensure rpcbind services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `rpcbind` utility maps RPC services to the ports on which they listen. RPC processes notify `rpcbind` when they start, registering the ports they are listening on and the RPC program numbers they expect to serve. The client system then contacts `rpcbind` on the server with a particular RPC program number. The `rpcbind.service` redirects the client to the proper port number so it can communicate with the requested service.

Portmapper is an RPC service, which always listens on tcp and udp 111, and is used to map other RPC services (such as nfs, nlockmgr, quotad, mountd, etc.) to their corresponding port number on the server. When a remote host makes an RPC call to that server, it first consults with portmap to determine where the RPC server is listening.

### **Rationale:**

A small request (~82 bytes via UDP) sent to the Portmapper generates a large response (7x to 28x amplification), which makes it a suitable tool for DDoS attacks. If `rpcbind` is not required, it is recommended to remove `rpcbind` package to reduce the potential attack surface.

### **Impact:**

Many of the libvirt packages used by Enterprise Linux virtualization, and the `nfs-utils` package used for The Network File System (NFS), are dependent on the `rpcbind` package. If the `rpcbind` package is removed, these dependent packages will be removed as well. Before removing the `rpcbind` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `rpcbind.socket` and `rpcbind.service` leaving the `rpcbind` package installed.

## Audit:

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

```
# dpkg-query -s rpcbind &>/dev/null && echo "rpcbind is installed"
```

Nothing should be returned.

- OR -

- IF - the `rpcbind` package is required as a dependency:

Run the following command to verify `rpcbind.socket` and `rpcbind.service` are not enabled:

```
# systemctl is-enabled rpcbind.socket rpcbind.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify `rpcbind.socket` and `rpcbind.service` are not active:

```
# systemctl is-active rpcbind.socket rpcbind.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `rpcbind.socket` and `rpcbind.service`, and remove the `rpcbind` package:

```
# systemctl stop rpcbind.socket rpcbind.service
# apt purge rpcbind
```

- OR -

- IF - the `rpcbind` package is required as a dependency:

Run the following commands to stop and mask the `rpcbind.socket` and `rpcbind.service`:

```
# systemctl stop rpcbind.socket rpcbind.service
# systemctl mask rpcbind.socket rpcbind.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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, T1498, T1498.002, T1543, T1543.002	TA0008	M1042

## *2.1.13 Ensure rsync services are not in use (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:**

`rsync.service` presents a security risk as the `rsync` protocol is unencrypted.

The `rsync` package should be removed to reduce the attack area of the system.

### **Impact:**

There may be packages that are dependent on the `rsync` package. If the `rsync` package is removed, these dependent packages will be removed as well. Before removing the `rsync` package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask `rsync.service` leaving the `rsync` package installed.

## Audit:

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

```
# dpkg-query -s rsync &>/dev/null && echo "rsync is installed"
```

Nothing should be returned.

- OR -

- IF - the `rsync` package is required as a dependency:

Run the following command to verify `rsync.service` is not enabled:

```
# systemctl is-enabled rsync.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify `rsync.service` is not active:

```
# systemctl is-active rsync.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `rsync.service`, and remove the `rsync` package:

```
# systemctl stop rsync.service  
# apt purge rsync
```

- OR -

- IF - the `rsync` package is required as a dependency:

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

```
# systemctl stop rsync.service  
# systemctl mask rsync.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

## *2.1.14 Ensure samba file server services are not in use (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.

### **Impact:**

There may be packages that are dependent on the `samba` package. If the `samba` package is removed, these dependent packages will be removed as well. Before removing the `samba` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `smbd.service` leaving the `samba` package installed.

## Audit:

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

```
# dpkg-query -s samba >/dev/null && echo "samba is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify `smbd.service` is not enabled:

```
# systemctl is-enabled smbd.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify the `smbd.service` is not active:

```
# systemctl is-active smbd.service 2>/dev/null | grep '^active'
```

Nothing should be returned

## Remediation:

Run the following commands to stop `smbd.service` and remove `samba` package:

```
# systemctl stop smbd.service
# apt purge samba
```

- OR -

- IF - the `samba` package is required as a dependency:

Run the following commands to stop and mask the `smbd.service`:

```
# systemctl stop smbd.service
# systemctl mask smbd.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b></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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b></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	

## 2.1.15 Ensure snmp services are not in use (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 `snmpd` 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.

### Impact:

There may be packages that are dependent on the `snmpd` package. If the `snmpd` package is removed, these packages will be removed as well.

Before removing the `snmpd` package, review any dependent packages to determine if they are required on the system. If a dependent package is required, stop and mask the `snmpd.service` leaving the `snmpd` package installed.

## Audit:

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

```
# dpkg-query -s snmpd &>/dev/null && echo "snmpd is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify the `snmpd.service` is not enabled:

```
# systemctl is-enabled snmpd.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify the `snmpd.service` is not active:

```
# systemctl is-active snmpd.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `snmpd.service` and remove the `snmpd` package:

```
# systemctl stop snmpd.service
# apt purge snmpd
```

- OR - If the package is required for dependencies:

Run the following commands to stop and mask the `snmpd.service`:

```
# systemctl stop snmpd.service
# systemctl mask snmpd.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

## *2.1.16 Ensure tftp server services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files.

### **Rationale:**

Unless there is a need to run the system as a TFTP server, it is recommended that the package be removed to reduce the potential attack surface.

TFTP does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to exploit TFTP to gain access to files

### **Impact:**

TFTP is often used to provide files for network booting such as for PXE based installation of servers.

There may be packages that are dependent on the `tftpd-hpa` package. If the `tftpd-hpa` package is removed, these dependent packages will be removed as well. Before removing the `tftpd-hpa` package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask `tftpd-hpa.service` leaving the `tftpd-hpa` package installed.

## Audit:

Run the following command to verify `tftpd-hpa` is not installed:

```
# dpkg-query -s tftpd-hpa &>/dev/null && echo "tftpd-hpa is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify `tftpd-hpa.service` is not enabled:

```
# systemctl is-enabled tftpd-hpa.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify the `tftpd-hpa.service` is not active:

```
# systemctl is-active tftpd-hpa.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `tftpd-hpa.service`, and remove the `tftpd-hpa` package:

```
# systemctl stop tftpd-hpa.service  
# apt purge tftpd-hpa
```

- OR -

- IF - the `tftpd-hpa` package is required as a dependency:

Run the following commands to stop and mask `tftpd-hpa.service`:

```
# systemctl stop tftpd-hpa.service  
# systemctl mask tftpd-hpa.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

## *2.1.17 Ensure web proxy server services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Squid is a standard proxy server used in many distributions and environments.

### **Rationale:**

Unless a system is specifically set up to act as a proxy server, it is recommended that the squid package be removed to reduce the potential attack surface.

**Note:** Several HTTP proxy servers exist. These should be checked and removed unless required.

### **Impact:**

There may be packages that are dependent on the `squid` package. If the `squid` package is removed, these dependent packages will be removed as well. Before removing the `squid` package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the `squid.service` leaving the `squid` package installed.

## Audit:

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

```
# dpkg-query -s squid &>/dev/null && echo "squid is installed"
```

Nothing should be returned.

- OR -

- IF - the package is required for dependencies:

Run the following command to verify `squid.service` is not enabled:

```
# systemctl is-enabled squid.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify the `squid.service` is not active:

```
# systemctl is-active squid.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `squid.service` and remove the `squid` package:

```
# systemctl stop squid.service
# apt purge squid
```

- OR - If the `squid` package is required as a dependency:

Run the following commands to stop and mask the `squid.service`:

```
# systemctl stop squid.service
# systemctl mask squid.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## Additional Information:

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

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

## *2.1.18 Ensure web server services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Web servers provide the ability to host web site content.

### **Rationale:**

Unless there is a local site approved requirement to run a web server service on the system, web server packages should be removed to reduce the potential attack surface.

### **Impact:**

Removal of web server packages will remove that ability for the server to host web services.

- IF - the web server package is required for a dependency, any related service or socket should be stopped and masked.

**Note:** If the remediation steps to mask a service are followed and that package is not installed on the system, the service and/or socket will still be masked. If the package is installed due to an approved requirement to host a web server, the associated service and/or socket would need to be unmasked before it could be enabled and/or started.

## Audit:

Run the following command to verify `apache2` is not installed:

```
# dpkg-query -s apache2 &>/dev/null && echo "apache2 is installed"
```

Nothing should be returned.

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

```
# dpkg-query -s nginx &>/dev/null && echo "nginx is installed"
```

Nothing should be returned.

- OR -

- IF - a package is installed **and** is required for dependencies:

Run the following command to verify `apache2.socket`, `apache2.service`, and `nginx.service` are not enabled:

```
# systemctl is-enabled apache2.socket apache2.service nginx.service  
2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify `apache2.socket`, `apache2.service`, and `nginx.service` are not active:

```
# systemctl is-active apache2.socket apache2.service nginx.service  
2>/dev/null | grep '^active'
```

Nothing should be returned

## Note:

- Other web server packages may exist. They should also be audited, if not required and authorized by local site policy
- If the package is required for a dependency:
  - Ensure the dependent package is approved by local site policy
  - Ensure stopping and masking the service and/or socket meets local site policy

## **Remediation:**

Run the following commands to stop `httpd.socket`, `httpd.service`, and `nginx.service`, and remove `httpd` and `nginx` packages:

```
# systemctl stop apache2.socket httpd.service nginx.service  
# apt purge apache2 nginx
```

**- OR -**

**- IF -** a package is installed **and** is required for dependencies:

Run the following commands to stop and mask `apache2.socket`, `apache2.service`, and `nginx.service`:

```
# systemctl stop apache2.socket apache2.service nginx.service  
# systemctl mask apache2.socket apache2.service nginx.service
```

**Note:** Other web server packages may exist. If not required and authorized by local site policy, they should also be removed. If the package is required for a dependency, the service and socket should be stopped and masked.

## **References:**

1. NIST SP 800-53 Rev. 5: CM-7

## **Additional Information:**

Several `httpd` servers exist and can use other service names. `apache2` and `nginx` are example services that provide an HTTP server. These and other services should also be audited

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> 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:**

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

## *2.1.19 Ensure xinetd services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **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:**

There may be packages that are dependent on the `xinetd` package. If the `xinetd` package is removed, these dependent packages will be removed as well. Before removing the `xinetd` package, review any dependent packages to determine if they are required on the system.

**-IF-** a dependent package is required: stop and mask `xinetd.service` leaving the `xinetd` package installed.

## Audit:

Run the following command to verify the `xinetd` package is not installed:

```
# dpkg-query -s xinetd &>/dev/null && echo "xinetd is installed"
```

Nothing should be returned.

-OR-

-IF- the `xinetd` package is required as a dependency:

Run the following command to verify `xinetd.service` is not enabled:

```
# systemctl is-enabled xinetd.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify `xinetd.service` is not active:

```
# systemctl is-active xinetd.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `xinetd.service`, and remove the `xinetd` package:

```
# systemctl stop xinetd.service  
# apt purge xinetd
```

-OR-

-IF- the `xinetd` package is required as a dependency:

Run the following commands to stop and mask the `xinetd.service`:

```
# systemctl stop xinetd.service  
# systemctl mask xinetd.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

## *2.1.20 Ensure X window server services are not in use (Automated)*

### **Profile Applicability:**

- Level 2 - 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:**

If a Graphical Desktop Manager (GDM) is in use on the system, there may be a dependency on the `xorg-x11-server-common` package. If the GDM is required and approved by local site policy, the package should **not** be removed.

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.

### **Audit:**

- IF - a Graphical Desktop Manager or X-Windows server is not required and approved by local site policy:

Run the following command to Verify X Windows Server is not installed.

```
dpkg-query -s xserver-common &>/dev/null && echo "xserver-common is installed"
```

Nothing should be returned

## **Remediation:**

- IF - a Graphical Desktop Manager or X-Windows server is not required and approved by local site policy:

Run the following command to remove the X Windows Server package:

```
# apt purge xserver-common
```

## **References:**

1. NIST SP 800-53 Rev. 5: CM-11

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>2.6 Address unapproved software</b> 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

## *2.1.21 Ensure mail transfer agent is configured for local-only mode (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.

### **Rationale:**

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

## Audit:

Run the following script to verify that the MTA is not listening on any non-loopback address ( 127.0.0.1 or ::1

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

{
l_output=""
l_output2=""
a_port_list=("25" "465" "587")

# Check if inet_interfaces is not set to all
if [ "$(postconf -n inet_interfaces)" != "inet_interfaces = all" ]; then
    for l_port_number in "${a_port_list[@]}"; do
        if ss -plntu | grep -P -- ":""$l_port_number"\b' | grep -Pvq --
'\h+(127\.0\.0\.1|[\?::1\]?):'"$l_port_number"\b'; then
            l_output2="$l_output2\n - Port \"$l_port_number\" is listening on
a non-loopback network interface"
        else
            l_output="$l_output\n - Port \"$l_port_number\" is not listening
on a non-loopback network interface"
        fi
    done
else
    l_output2="$l_output2\n - Postfix is bound to all interfaces"
fi

unset a_port_list

# Provide output from checks
if [ -z "$l_output2" ]; then
    echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
else
    # If error output (l_output2) is not empty, we fail. Also output anything
    # that's correctly configured
    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:**

Edit `/etc/postfix/main.cf` and add the following line to the RECEIVING MAIL section. If the line already exists, change it to look like the line below:

```
inet_interfaces = loopback-only
```

Run the following command to restart `postfix`:

```
# systemctl restart postfix
```

## **Note:**

- This recommendation is designed around the postfix mail server.
- Depending on your environment you may have an alternative MTA installed such as exim4. If this is the case consult the documentation for your installed MTA to configure the recommended state.

## **References:**

1. NIST SP 800-53 Rev. 5: CM-7

## **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
T1018, T1018.000, T1210, T1210.000	TA0008	M1042

## *2.1.22 Ensure only approved services are listening on a network interface (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.

### **Impact:**

There may be packages that are dependent on the service's package. If the service's package is removed, these dependent packages will be removed as well. Before removing the service's package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `<service_name>.socket` and `<service_name>.service` leaving the service's package installed.

## Audit:

Run the following command:

```
# ss -plntu
```

Review the output to ensure:

- All services listed are required on the system and approved by local site policy.
- Both the port and interface the service is listening on are approved by local site policy.
- If a listed service is not required:
  - Remove the package containing the service
  - - IF - the service's package is required for a dependency, stop and mask the service and/or socket

## Remediation:

Run the following commands to stop the service and remove the package containing the service:

```
# systemctl stop <service_name>.socket <service_name>.service  
# apt purge <package_name>
```

- OR - If required packages have a dependency:

Run the following commands to stop and mask the service and socket:

```
# systemctl stop <service_name>.socket <service_name>.service  
# systemctl mask <service_name>.socket <service_name>.service
```

**Note:** replace <service\_name> with the appropriate service name.

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> 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:**

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

## 2.2 Configure Client Services

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

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

## *2.2.1 Ensure NIS Client is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client was used to bind a machine to an NIS server and receive the distributed configuration files.

### **Rationale:**

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

### **Impact:**

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

### **Audit:**

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

```
# dpkg-query -s nis &>/dev/null && echo "nis is installed"
```

Nothing should be returned.

### **Remediation:**

Uninstall `nis`:

```
# apt purge nis
```

### **References:**

1. NIST SP 800-53 Rev. 5: CM-7, CM-11

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>2.6 Address unapproved software</b>            Ensure that unauthorized software is either removed or the inventory is updated in a timely manner</p>	●	●	●

## MITRE ATT&CK Mappings:

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

## *2.2.2 Ensure rsh client is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the `rsh-client` 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-query -s rsh-client &>/dev/null && echo "rsh-client is installed"
```

Nothing should be returned.

### **Remediation:**

Uninstall `rsh`:

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

### **References:**

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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, T1203, T1203.000, T1543, T1543.002	TA0008	M1041, M1042

## *2.2.3 Ensure talk client is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

### **Impact:**

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required, it is advisable to remove the clients after use to prevent accidental or intentional misuse.

### **Audit:**

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

```
# dpkg-query -s talk &>/dev/null && echo "talk is installed"
```

Nothing should be returned.

### **Remediation:**

Uninstall `talk`:

```
# apt purge talk
```

### **References:**

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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, T1543, T1543.002	TA0006, TA0008	M1041, M1042

## *2.2.4 Ensure telnet client is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `telnet` package contains the `telnet` client, which allows users to start connections to other systems via the telnet protocol.

### **Rationale:**

The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The `ssh` package provides an encrypted session and stronger security and is included in most Linux distributions.

### **Impact:**

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

### **Audit:**

Verify `telnet` is not installed. Use the following command to provide the needed information:

```
# dpkg-query -s telnet &>/dev/null && echo "telnet is installed"
```

Nothing should be returned.

### **Remediation:**

Uninstall `telnet`:

```
# apt purge telnet
```

### **References:**

1. NIST SP 800-53 Rev. 5: CM-7, CM-11

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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, T1203, T1203.000, T1543, T1543.002	TA0006, TA0008	M1041, M1042

## *2.2.5 Ensure ldap client is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

### **Rationale:**

If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.

### **Impact:**

Removing the LDAP client will prevent or inhibit using LDAP for authentication in your environment.

### **Audit:**

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

```
# dpkg-query -s ldap-utils &>/dev/null && echo "ldap-utils is installed"
```

Nothing should be returned.

### **Remediation:**

Uninstall `ldap-utils`:

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

### **References:**

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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, T1543, T1543.002	TA0008	M1042

## *2.2.6 Ensure ftp client is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

FTP (File Transfer Protocol) is a traditional and widely used standard tool for transferring files between a server and clients over a network, especially where no authentication is necessary (permits anonymous users to connect to a server).

### **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 removed to reduce the potential attack surface.

### **Audit:**

Verify `ftp` is not installed. Use the following command to provide the needed information:

```
# dpkg-query -s ftp &>/dev/null && echo "ftp is installed"
```

Nothing should be returned.

### **Remediation:**

Run the following command to uninstall `ftp`:

```
# apt purge ftp
```

### **References:**

1. NIST SP 800-53 Rev. 5: CM-7, CM-11

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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, T1543, T1543.002	TA0008	M1042

## 2.3 Configure Time Synchronization

It is recommended that systems be configured to synchronize their time using a service such as `systemd-timesyncd`, or `chrony`.

Virtual systems may be configured to receive their time synchronization from their host system.

The host system must be configured to synchronize its time from an authoritative source to be considered compliant with this section.

Any "physical" clock present on a system should be synchronized from an authoritative time source.

**Only one time synchronization method should be in use on the system**

**Notes:** 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

### **2.3.1 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`, or `chrony`.

### *2.3.1.1 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.

#### **Notes:**

- 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 two time synchronization daemons should be available; `chrony` or `systemd-timesyncd`

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

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    service_not_enabled_chk()
    {
        l_out2=""
        if systemctl is-enabled "$l_service_name" 2>/dev/null | grep -q 'enabled'; then
            l_out2="$l_out2\n - Daemon: \"$l_service_name\" is enabled on the system"
        fi
        if systemctl is-active "$l_service_name" 2>/dev/null | grep -q '^active'; then
            l_out2="$l_out2\n - Daemon: \"$l_service_name\" is active on the system"
        fi
    }
    l_service_name="systemd-timesyncd.service" # Check systemd-timesyncd daemon
    service_not_enabled_chk
    if [ -n "$l_out2" ]; then
        l_timesyncd="y"
        l_out_ts=$l_out2
    else
        l_timesyncd="n"
        l_out_ts="\n - Daemon: \"$l_service_name\" is not enabled and not active on the system"
    fi
    l_service_name="chrony.service" # Check chrony
    service_not_enabled_chk
    if [ -n "$l_out2" ]; then
        l_chrony="y"
        l_out_chrony="$l_out2"
    else
        l_chrony="n"
        l_out_chrony="\n - Daemon: \"$l_service_name\" is not enabled and not active on the system"
    fi
    l_status="$l_timesyncd$l_chrony"
    case "$l_status" in
        yy)
            l_output2=" - More than one time sync daemon is in use on the system"
            l_out_ts=$l_out_chrony
            ;;
        nn)
            l_output2=" - No time sync daemon is in use on the system"
            l_out_ts=$l_out_chrony
            ;;
        yn|ny)
            l_output=" - Only one time sync daemon is in use on the system"
            l_out_ts=$l_out_chrony
            ;;
        *)
            l_output2=" - Unable to determine time sync daemon(s) status"
            l_out_ts=$l_out_chrony
            ;;
    esac

    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 - * Reasons for audit failure *\n:$l_output2\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 two time synchronization daemons; **chrony** (1) OR **systemd-timesyncd** (2) 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 mask systemd-timesyncd.service
```

**Note:**

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

### **2. systemd-timesyncd**

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

```
# apt purge chrony  
# apt autoremove chrony
```

**Note:**

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

## **References:**

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.4 Standardize Time Synchronization</b> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	<b>6.1 Utilize Three Synchronized Time Sources</b> 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	

## 2.3.2 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.

## Notes:

- 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 is 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**

### *2.3.2.1 Ensure systemd-timesyncd configured with authorized timeserver (Automated)*

#### **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:

Run the following command to verify the **NTP** **and/or** **FallbackNTP** option is set to local site approved authoritative time server(s):

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

{
    l_output="" l_output2=""
    a_parlist=("$NTP=[^#\n\r]+\"FallbackNTP=[^#\n\r]+")
    l_systemd_config_file="/etc/systemd/timesyncd.conf" # Main systemd configuration file
    config_file_parameter_chk()
    {
        unset A_out; declare -A A_out # Check config file(s) setting
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out##*/# }"
                else
                    l_systemd_parameter=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    grep -Piq -- "^\h*$l_systemd_parameter\b" <<< "$l_systemd_parameter" &&
A_out+=(["$l_systemd_parameter"]="$l_file")
                fi
            fi
        done < <(/usr/bin/systemd-analyze cat-config "$l_systemd_config_file" | grep -Po
'^\h*([^\n\r]+|\h*[^\n\r\h]+\.\conf\b)')
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="=" read -r l_systemd_file_parameter_name l_systemd_file_parameter_value; do
                l_systemd_file_parameter_name="${l_systemd_file_parameter_name// /}"
                l_systemd_file_parameter_value="${l_systemd_file_parameter_value// /}"
                if grep -Piq "^\h*$l_systemd_file_parameter_value\b" <<<
"$l_systemd_file_parameter_value"; then
                    l_output="$l_output\n - \"\$l_systemd_file_parameter_name\" is correctly set to
\"\$l_systemd_file_parameter_value\" in \"$(printf '%s' \"${A_out[@]}\")\"\n"
                else
                    l_output2="$l_output2\n - \"\$l_systemd_file_parameter_name\" is incorrectly set to
\"\$l_systemd_file_parameter_value\" in \"$(printf '%s' \"${A_out[@]}\")\"\n" and should have a value
matching: \"\$l_systemd_file_parameter_value\"\n"
                fi
            done < <(grep -Po -- "^\h*$l_systemd_file_parameter_name\b=\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"\$l_systemd_file_parameter_name\" is not set in an included file\n"
            ** Note: \"\$l_systemd_file_parameter_name\" May be set in a file that's ignored by load procedure
            **\n"
        fi
    }
    while IFS="=" read -r l_systemd_parameter_name l_systemd_parameter_value; do # Assess and
check parameters
        l_systemd_parameter_name="${l_systemd_parameter_name// /}"
        l_systemd_parameter_value="${l_systemd_parameter_value// /}"
        config_file_parameter_chk
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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 "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}
```

*Example output:*

```
- Audit Result:  
  ** PASS **  
  
- "NTP" is correctly set to "time.nist.gov" in "/etc/systemd/timesyncd.conf"  
  
- "FallbackNTP" is correctly set to "time-a-g.nist.gov" in  
"/etc/systemd/timesyncd.conf"
```

**Remediation:**

Set `NTP` and/or `FallbackNTP` parameters to local site approved authoritative time server(s) in `/etc/systemd/timesyncd.conf` or a file in `/etc/systemd/timesyncd.conf.d/` ending in `.conf` in the `[Time]` section:

*Example file:*

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

*Example script to create systemd drop-in file:*

```
#!/usr/bin/env bash  
  
{  
  [ ! -d /etc/systemd/timesyncd.conf.d/ ] && mkdir  
  /etc/systemd/timesyncd.conf.d/  
  printf '%s\n' "[Time]" "NTP=time.nist.gov" "FallbackNTP=time-a-g.nist.gov  
time-b-g.nist.gov time-c-g.nist.gov" >> /etc/systemd/timesyncd.conf.d/60-  
timesyncd.conf  
}
```

**Note:** If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run the following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

**Default Value:**

`#NTP=`

`#FallbackNTP=`

**References:**

1. <https://www.freedesktop.org/software/systemd/man/timesyncd.conf.html>
2. <https://tf.nist.gov/tf-cgi/servers.cgi>
3. NIST SP 800-53 Rev. 5: AU-7, AU-8

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.4 Standardize Time Synchronization</b> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.</p>		●	●
v7	<p><b>6.1 Utilize Three Synchronized Time Sources</b> 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, T1562, T1562.001	TA0002	M1022

## *2.3.2.2 Ensure systemd-timesyncd is enabled and running (Manual)*

### **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
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-7, AU-8

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.4 Standardize Time Synchronization</b> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	<b>6.1 Utilize Three Synchronized Time Sources</b> 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

### 2.3.3 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/>.

#### Notes:

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

### *2.3.3.1 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 script to ensure `chrony` is configured with authorized timeserver:

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

{
    l_output=""
    l_output2=""
    a_parlist=(^\\h*(server|pool)\\h+\\H+")
    l_chrony_config_dir="/etc/chrony" # Chrony configuration directory
    config_file_parameter_chk() {
        unset A_out
        declare -A A_out
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_chrony_parameter=$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    A_out+=(["$l_chrony_parameter"]="$l_file")
                fi
            fi
        done < <(find "$l_chrony_config_dir" -name '*.conf' -exec systemd-analyze cat-config {} + | grep -Pio '^\\h*([^\n\r]+|\\h*/[^\\n\r\\h]+\.\conf\b)')
        if (( ${#A_out[@]} > 0 )); then
            for l_chrony_parameter in "${!A_out[@]}"; do
                l_file="${A_out[$l_chrony_parameter]}"
                l_output="$l_output\\n - \"$l_chrony_parameter\" is set in \"$l_file\"\\n"
            done
        else
            l_output2="$l_output2\\n - No 'server' or 'pool' settings found in Chrony configuration files\\n"
        fi
    }
    for l_chrony_parameter_regex in "${a_parlist[@]}"; do
        config_file_parameter_chk
    done

    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:**

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  
# apt autoremove chrony
```

## **References:**

1. `chrony.conf(5)` Manual Page
2. <https://tf.nist.gov/tf-cgi/servers.cgi>
3. NIST SP 800-53 Rev. 5: AU-3, AU-12

## **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	<p><b>8.4 Standardize Time Synchronization</b> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.</p>		●	●
v7	<p><b>6.1 Utilize Three Synchronized Time Sources</b> 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, T1562, T1562.001	TA0002	M1022

### *2.3.3.2 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 privileges

#### **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
# apt autoremove chrony
```

#### **Default Value:**

`user _chrony`

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-8

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.4 Standardize Time Synchronization</b> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.</p>		●	●
v7	<p><b>6.1 Utilize Three Synchronized Time Sources</b> 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, T1562, T1562.001	TA0002	M1022

### *2.3.3.3 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  
# apt autoremove chrony
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-8

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.4 Standardize Time Synchronization</b> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	<b>6.1 Utilize Three Synchronized Time Sources</b> 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

## **2.4 Job Schedulers**

A job scheduler is used to execute jobs, commands, or shell scripts, at fixed times, dates, or intervals

## 2.4.1 Configure cron

`cron` is a time based job scheduler

**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
- **-IF-** `cron` is not installed on the system, this sub section can be skipped

## 2.4.1.1 Ensure cron daemon is enabled and active (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `cron` daemon is used to execute batch jobs on the system.

### Rationale:

While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and `cron` is used to execute them.

### Audit:

- IF - cron is installed on the system:

Run the following command to verify `cron` is enabled:

```
# systemctl list-unit-files | awk '$1~/^crond?\!.service/{print $2}'  
enabled
```

Run the following command to verify that `cron` is active:

```
# systemctl list-units | awk '$1~/^crond?\!.service/{print $3}'  
active
```

### Remediation:

- IF - cron is installed on the system:

Run the following commands to unmask, enable, and start `cron`:

```
# systemctl unmask "$(systemctl list-unit-files | awk  
'$1~/^crond?\!.service/{print $1}')"  
# systemctl --now enable "$(systemctl list-unit-files | awk  
'$1~/^crond?\!.service/{print $1}')"
```

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**MITRE ATT&CK Mappings:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1562, T1562.001	TA0005	M1018

## *2.4.1.2 Ensure permissions on /etc/crontab are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/crontab` file is used by `cron` to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file.

### **Rationale:**

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

### **Audit:**

- IF - cron is installed on the system:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group or other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/crontab
Access: (600/-rw-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

### **Remediation:**

- IF - cron is installed on the system:

Run the following commands to set ownership and permissions on `/etc/crontab`:

```
# chown root:root /etc/crontab
# chmod og-rwx /etc/crontab
```

### **Default Value:**

Access: (644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1053, T1053.003	TA0002, TA0007	M1018

### *2.4.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

This directory contains system `cron` jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

#### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

#### **Audit:**

##### **- IF - cron is installed on the system:**

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.hourly/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

#### **Remediation:**

##### **- IF - cron is installed on the system:**

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/
```

#### **Default Value:**

Access: (755/drwxr-xr-x) Uid: ( 0/ root) Gid: ( 0/ root)

#### **References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1053, T1053.003	TA0002, TA0007	M1018

## *2.4.1.4 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 daily. The files in this directory cannot be manipulated by the `crontab` command but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### **Audit:**

#### **- IF - cron is installed on the system:**

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.daily/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

### **Remediation:**

#### **- IF - cron is installed on the system:**

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/
```

### **Default Value:**

Access: (755/drwxr-xr-x) Uid: ( 0/ root) Gid: ( 0/ root)

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1053, T1053.003	TA0002, TA0007	M1018

## *2.4.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/cron.weekly` directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the `crontab` command but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### **Audit:**

#### **- IF - cron is installed on the system:**

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.weekly/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

### **Remediation:**

#### **- IF - cron is installed on the system:**

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/
```

### **Default Value:**

`Access: (755/drwxr-xr-x) Uid: ( 0/ root) Gid: ( 0/ root)`

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1053, T1053.003	TA0002, TA0007	M1018

## *2.4.1.6 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 monthly. The files in this directory cannot be manipulated by the `crontab` command but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### **Audit:**

#### **- IF - cron is installed on the system:**

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.monthly/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

### **Remediation:**

#### **- IF - cron is installed on the system:**

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/
```

### **Default Value:**

`Access: (755/drwxr-xr-x) Uid: ( 0/ root) Gid: ( 0/ root)`

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1053, T1053.003	TA0002, TA0007	M1018

## *2.4.1.7 Ensure permissions on /etc/cron.d are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/cron.d` directory contains system `cron` jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from `/etc/crontab`, but require more granular control as to when they run. The files in this directory cannot be manipulated by the `crontab` command but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### **Audit:**

#### **- IF - cron is installed on the system:**

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.d/
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

### **Remediation:**

#### **- IF - cron is installed on the system:**

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/
```

### **Default Value:**

Access: (755/drwxr-xr-x) Uid: ( 0/ root) Gid: ( 0/ root)

**References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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

## *2.4.1.8 Ensure crontab is restricted to authorized users (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

`crontab` is the program used to install, deinstall, or list the tables used to drive the cron daemon. Each user can have their own crontab, and though these are files in `/var/spool/cron/crontabs`, they are not intended to be edited directly.

If the `/etc/cron.allow` file exists, then you must be listed (one user per line) therein in order to be allowed to use this command. If the `/etc/cron.allow` file does not exist but the `/etc/cron.deny` file does exist, then you must not be listed in the `/etc/cron.deny` file in order to use this command.

If neither of these files exists, then depending on site-dependent configuration parameters, only the super user will be allowed to use this command, or all users will be able to use this command.

If both files exist then `/etc/cron.allow` takes precedence. Which means that `/etc/cron.deny` is not considered and your user must be listed in `/etc/cron.allow` in order to be able to use the crontab.

Regardless of the existence of any of these files, the root administrative user is always allowed to set up a crontab.

The files `/etc/cron.allow` and `/etc/cron.deny`, if they exist, must be either world-readable, or readable by group `crontab`. If they are not, then cron will deny access to all users until the permissions are fixed.

There is one file for each user's crontab under the `/var/spool/cron/crontabs` directory. Users are not allowed to edit the files under that directory directly to ensure that only users allowed by the system to run periodic tasks can add them, and only syntactically correct crontabs will be written there. This is enforced by having the directory writable only by the `crontab` group and configuring crontab command with the setgid bit set for that specific group.

### **Note:**

- Even though a given user is not listed in `cron.allow`, cron jobs can still be run as that user
- The files `/etc/cron.allow` and `/etc/cron.deny`, if they exist, 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:

- IF - cron is installed on the system:

Run the following command to verify `/etc/cron.allow`:

- Exists
- Is mode 0640 or more restrictive
- Is owned by the user `root`
- Is group owned by the group `root`

```
# stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/cron.allow
Access: (640/-rw-r-----) Owner: (root) Group: (root)
```

Run the following command to verify either `cron.deny` doesn't exist or is:

- Mode 0640 or more restrictive
- Owned by the user `root`
- Group owned by the group `root`

```
# [ -e "/etc/cron.deny" ] && stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/cron.deny
else
```

Verify either nothing is returned or returned value is:

```
Access: (640/-rw-r-----) Owner: (root) Group: (root)
```

## **Remediation:**

- **IF** - cron is installed on the system:

Run the following script to:

- Create `/etc/cron.allow` if it doesn't exist
- Change owner to user `root`
- Change group owner to group `root`
- Change mode to `640` or more restrictive

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

{
    [ ! -e "/etc/cron.allow" ] && touch /etc/cron.allow
    chown root:root /etc/cron.allow
    chmod u-x,g-wx,o-rwx /etc/cron.allow
}
```

- **IF** - `/etc/cron.deny` exists, run the following commands to:

- Change owner to user `root`
- Change group owner to group `root`
- Change mode to `640` or more restrictive

```
# [ -e "/etc/cron.deny" ] && chown root:root /etc/cron.deny
# [ -e "/etc/cron.deny" ] && chmod u-x,g-wx,o-rwx /etc/cron.deny
```

## **References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1053, T1053.003	TA0002	M1018

## **2.4.2 Configure at**

`at` is a command-line utility used to schedule a job for later execution

**Note:** if `at` is not installed on the system, this section can be skipped

## *2.4.2.1 Ensure at is restricted to authorized users (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

`at` allows fairly complex time specifications, extending the POSIX.2 standard. It accepts times of the form HH:MM to run a job at a specific time of day. (If that time is already past, the next day is assumed.) You may also specify midnight, noon, or teatime (4pm) and you can have a time-of-day suffixed with AM or PM for running in the morning or the evening. You can also say what day the job will be run, by giving a date in the form month-name day with an optional year, or giving a date of the form MMDD[CC]YY, MM/DD/[CC]YY, DD.MM.[CC]YY or [CC]YY-MM-DD. The specification of a date must follow the specification of the time of day. You can also give times like now + count time-units, where the time-units can be minutes, hours, days, or weeks and you can tell `at` to run the job today by suffixing the time with today and to run the job tomorrow by suffixing the time with tomorrow.

The `/etc/at.allow` and `/etc/at.deny` files determine which user can submit commands for later execution via `at` or `batch`. The format of the files is a list of usernames, one on each line. Whitespace is not permitted. If the file `/etc/at.allow` exists, only usernames mentioned in it are allowed to use `at`. If `/etc/at.allow` does not exist, `/etc/at.deny` is checked, every username not mentioned in it is then allowed to use `at`. An empty `/etc/at.deny` means that every user may use `at`. If neither file exists, only the superuser is allowed to use `at`.

### **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:

-IF- at is installed on the system:

Run the following command to verify /etc/at.allow:

- Exists
- Is mode 0640 or more restrictive
- Is owned by the user root
- Is group owned by the group daemon or group root

```
# stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/at.allow
Access: (640/-rw-r-----) Owner: (root) Group: (daemon)
-OR-
Access: (640/-rw-r-----) Owner: (root) Group: (root)
```

Verify mode is 640 or more restrictive, owner is root, and group is daemon or root

Run the following command to verify at.deny doesn't exist, -OR- is:

- Mode 0640 or more restrictive
- Owned by the user root
- Group owned by the group daemon or group root

```
# [ -e "/etc/at.deny" ] && stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/at.deny
Access: (640/-rw-r-----) Owner: (root) Group: (daemon)
-OR-
Access: (640/-rw-r-----) Owner: (root) Group: (root)
-OR-
Nothing is returned
```

If a value is returned, Verify mode is 640 or more restrictive, owner is root, and group is daemon or root

## Remediation:

-IF- at is installed on the system:

Run the following script to:

- /etc/at.allow:
  - Create the file if it doesn't exist
  - Change owner or user root
  - If group daemon exists, change to group daemon, else change group to root
  - Change mode to 640 or more restrictive
- -IF- /etc/at.deny exists:
  - Change owner or user root
  - If group daemon exists, change to group daemon, else change group to root
  - Change mode to 640 or more restrictive

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

{
    grep -Pq -- '^daemon\b' /etc/group && l_group="daemon" || l_group="root"
    [ ! -e "/etc/at.allow" ] && touch /etc/at.allow
    chown root:$l_group /etc/at.allow
    chmod u-x,g-wx,o-rwx /etc/at.allow
    [ -e "/etc/at.deny" ] && chown root:$l_group /etc/at.deny
    [ -e "/etc/at.deny" ] && chmod u-x,g-wx,o-rwx /etc/at.deny
}
```

## References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1053, T1053.003	TA0002	M1018

## **3 Network**

This section provides guidance on for securing the network configuration of the system

### **3.1 Configure Network Devices**

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

**Note:** This should not be considered a comprehensive list, you may wish to consider additions to those listed here for your environment.

### *3.1.1 Ensure IPv6 status is identified (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 trillion<sup>3</sup> 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.

**Note:** It is recommended that IPv6 be enabled and configured unless this is against local site policy

#### **Impact:**

IETF RFC 4038 recommends that applications are built with an assumption of dual stack.

When enabled, IPv6 will require additional configuration to reduce risk to the system.

## Audit:

Run the following to identify if IPv6 is enabled on the system:

```
# grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && echo -e "\n -\nIPv6 is enabled\n" || echo -e "\n -\nIPv6 is not enabled\n"
```

## Remediation:

Enable or disable IPv6 in accordance with system requirements and local site policy

## Default Value:

IPv6 is enabled

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## 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.

## 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:**

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

### *3.1.2 Ensure wireless interfaces are disabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server

#### **Description:**

Wireless networking is used when wired networks are unavailable.

#### **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:

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    module_chk()
    {
        # Check how module will be loaded
        l_loadable=$(modprobe -n -v "$l_mname")
        if grep -Pq -- '^h*install \ /bin\/(true|false)' <<< "$l_loadable";
    then
        l_output="$l_output\n - module: \"$l_mname\" is not loadable:
\"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable:
\"$l_loadable\""
        fi
        # Check is the module currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
        # Check if the module is deny listed
        if modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mname\b";
    then
        l_output="$l_output\n - module: \"$l_mname\" is deny listed in:
\"$(grep -Pl -- "^\h*blacklist\h+$l_mname\b" /etc/modprobe.d/*)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    if [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
        l_dname=$(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 l_mname in $l_dname; do
            module_chk
        done
    fi
    # Report results. If no failures output in l_output2, we pass
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n  ** PASS **"
        if [ -z "$l_output" ]; then
            echo -e "\n - System has no wireless NICs installed"
        else
            echo -e "\n$l_output\n"
        fi
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

Run the following script to disable any wireless interfaces:

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

{
    module_fix()
    {
        if ! modprobe -n -v "$l_mname" | grep -P -- '^h*install
\bin\/(true|false)'; then
            echo -e " - setting module: \"$l_mname\" to be un-loadable"
            echo -e "install $l_mname /bin/false" >>
/etc/modprobe.d/"$l_mname".conf
        fi
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e " - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
        if ! grep -Pq -- '^h*blacklist\h+$l_mname\b' /etc/modprobe.d/*; then
            echo -e " - deny listing \"$l_mname\""
            echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mname".conf
        fi
    }
    if [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
        l_dname=$(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 l_mname in $l_dname; do
            module_fix
        done
    fi
}
```

## **References:**

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>15.4 Disable Wireless Access on Devices if Not Required</b>            Disable wireless access on devices that do not have a business purpose for wireless access.</p>	●	●	●
v7	<p><b>15.5 Limit Wireless Access on Client Devices</b>            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.</p>	●	●	●

## MITRE ATT&CK Mappings:

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

### *3.1.3 Ensure bluetooth services are not in use (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 2 - Workstation

#### **Description:**

Bluetooth is a short-range wireless technology standard that is used for exchanging data between devices over short distances. It employs UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz. It is mainly used as an alternative to wire connections.

#### **Rationale:**

An attacker may be able to find a way to access or corrupt your data. One example of this type of activity is `bluesnarfing`, which refers to attackers using a Bluetooth connection to steal information off of your Bluetooth device. Also, viruses or other malicious code can take advantage of Bluetooth technology to infect other devices. If you are infected, your data may be corrupted, compromised, stolen, or lost.

#### **Impact:**

Many personal electronic devices (PEDs) use Bluetooth technology. For example, you may be able to operate your computer with a wireless keyboard. Disabling Bluetooth will prevent these devices from connecting to the system.

There may be packages that are dependent on the `bluez` package. If the `bluez` package is removed, these dependent packages will be removed as well. Before removing the `bluez` package, review any dependent packages to determine if they are required on the system.

**-IF-** a dependent package is required: stop and mask `bluetooth.service` leaving the `bluez` package installed.

## Audit:

Run the following command to verify the `bluez` package is not installed:

```
# dpkg-query -s bluez >/dev/null && echo "bluez is installed"
```

Nothing should be returned.

- OR -

- IF - the `bluez` package is required as a dependency:

Run the following command to verify `bluetooth.service` is not enabled:

```
# systemctl is-enabled bluetooth.service 2>/dev/null | grep 'enabled'
```

Nothing should be returned

Run the following command to verify `bluetooth.service` is not active:

```
# systemctl is-active bluetooth.service 2>/dev/null | grep '^active'
```

Nothing should be returned

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop `bluetooth.service`, and remove the `bluez` package:

```
# systemctl stop bluetooth.service  
# apt purge bluez
```

- OR -

- IF - the `bluez` package is required as a dependency:

Run the following commands to stop and mask `bluetooth.service`:

```
# systemctl stop bluetooth.service  
# systemctl mask bluetooth.service
```

**Note:** A reboot may be required

## References:

1. <https://www.cisa.gov/tips/st05-015>
2. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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
T1011, T1011.001	TA0010	M1042

## 3.2 Configure Network Kernel Modules

The Linux kernel modules support several network protocols that are not commonly used. If these protocols are not needed, it is recommended that they be disabled in the kernel.

**Note:** This should not be considered a comprehensive list of uncommon network protocols, you may wish to consider additions to those listed here for your environment.

### *3.2.1 Ensure dccp kernel module is not available (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 script to verify the `dccp` module is disabled:

-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
    l_mname="dccp" # set module name
    l_mttype="net" # set module type
    l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
    l_mpath="/lib/modules/**/kernel/$l_mttype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable=$(grep -P --
"^(h*install\b\$l_mname\b)" <<< "$l_loadable")
        if grep -Pq -- '^h*install \/bin/(true|false)' <<< "$l_loadable"; then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
        fi
    }
    module_loaded_chk()
    {
        # Check if the module is currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
    }
    module_deny_chk()
    {
        # Check if the module is deny listed
        l_dl="y"
        if modprobe --showconfig | grep -Pq -- '^h*blacklist\b+'$l_mpname'\b'; then
            l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\b\$l_mname\b" $l_searchloc)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            l_output3="$l_output3\n - \"$l_mdir\""
            [ "$l_dl" != "y" ] && module_deny_chk
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mttype" ]; then
                module_loadable_chk
                module_loaded_chk
            fi
        else
            l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
        fi
    done
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_output3" ] && echo -e "\n\n-- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
    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:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

**Remediation:**

Run the following script to disable the `dccp` module:

-IF- the module is available in the running kernel:

- Create a file with `install dccp /bin/false` in the `/etc/modprobe.d/` directory
- Create a file with `blacklist dccp` in the `/etc/modprobe.d/` directory
- Unload `dccp` from the kernel

-IF- available in ANY installed kernel:

- Create a file with `blacklist dccp` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```

#!/usr/bin/env bash

{
    l_mname="dccp" # set module name
    l_mtype="net" # set module type
    l_mpath="/lib/modules/**/kernel/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_fix()
    {
        # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
        #/etc/modprobe.d
        l_loadable=$(modprobe -n -v "$l_mname")
        [ $(wc -l <<< "$l_loadable") -gt "1" ] && l_loadable=$(grep -P --
        "(\^h*install|\b\$l_mname)\b" <<< "$l_loadable")
        if ! grep -Pq -- '\^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            echo -e "\n - setting module: \"$l_mname\" to be not loadable"
            echo -e "install \$l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    module_loaded_fix()
    {
        # If the module is currently loaded, unload the module
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e "\n - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
    }
    module_deny_fix()
    {
        # If the module isn't deny listed, denylist the module
        if ! modprobe --showconfig | grep -Pq -- "\^h*blacklist\h+\$l_mpname\b"; then
            echo -e "\n - deny listing \"$l_mname\""
            echo -e "blacklist \$l_mname" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/\$l_mndir" ] && [ -n "$(ls -A \$l_mdir/\$l_mndir)" ]; then
            echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
            module_deny_fix
            if [ "\$l_mdir" = "/lib/modules/$(uname -r)/kernel/\$l_mtype" ]; then
                module_loadable_fix
                module_loaded_fix
            fi
        else
            echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
        fi
    done
    echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}

```

## References:

1. NIST SP 800-53 Rev. 5: SI-4, CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

### *3.2.2 Ensure tipc kernel module is not available (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 script to verify the `tipc` module is disabled:

-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
    l_mname="tipc" # set module name
    l_mttype="net" # set module type
    l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
    l_mpath="/lib/modules/**/kernel/$l_mttype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable=$(grep -P --
"^(h*install\b\$l_mname\b)" <<< "$l_loadable")
        if grep -Pq -- '^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
        fi
    }
    module_loaded_chk()
    {
        # Check if the module is currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
    }
    module_deny_chk()
    {
        # Check if the module is deny listed
        l_dl="y"
        if modprobe --showconfig | grep -Pq -- '^h*blacklist\b+'$l_mpname'\b'; then
            l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\b\$l_mname\b" $l_searchloc)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            l_output3="$l_output3\n - \"$l_mdir\""
            [ "$l_dl" != "y" ] && module_deny_chk
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mttype" ]; then
                module_loadable_chk
                module_loaded_chk
            fi
        else
            l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
        fi
    done
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_output3" ] && echo -e "\n\n-- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
    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:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

**Remediation:**

Run the following script to disable the `tipc` module:

-IF- the module is available in the running kernel:

- Create a file with `install tipc /bin/false` in the `/etc/modprobe.d/` directory
- Create a file with `blacklist tipc` in the `/etc/modprobe.d/` directory
- Unload `tipc` from the kernel

-IF- available in ANY installed kernel:

- Create a file with `blacklist tipc` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```

#!/usr/bin/env bash

{
    l_mname="tipc" # set module name
    l_mtype="net" # set module type
    l_mpath="/lib/modules/**/kernel/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_fix()
    {
        # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
        # /etc/modprobe.d
        l_loadable=$(modprobe -n -v "$l_mname")
        [ $(wc -l <<< "$l_loadable") -gt "1" ] && l_loadable=$(grep -P --
        "(\^h*install\b\$l_mname\b)" <<< "$l_loadable")
        if ! grep -Pq -- '\^h*install \b/bin\b/(true|false)' <<< "$l_loadable"; then
            echo -e "\n - setting module: \"$l_mname\" to be not loadable"
            echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    module_loaded_fix()
    {
        # If the module is currently loaded, unload the module
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e "\n - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
    }
    module_deny_fix()
    {
        # If the module isn't deny listed, denylist the module
        if ! modprobe --showconfig | grep -Pq -- "\^h*blacklist\b+$l_mpname\b"; then
            echo -e "\n - deny listing \"$l_mname\""
            echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
            module_deny_fix
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
                module_loadable_fix
                module_loaded_fix
            fi
        else
            echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
        fi
    done
    echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}

```

## References:

1. NIST SP 800-53 Rev. 5: SI-4, CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

### *3.2.3 Ensure rds kernel module is not available (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 script to verify the `rds` module is disabled:

-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
    l_mname="rds" # set module name
    l_mttype="net" # set module type
    l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
    l_mpath="/lib/modules/**/kernel/$l_mttype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable=$(grep -P --
"^(h*install\b\$l_mname\b)" <<< "$l_loadable")
        if grep -Pq -- '^h*install \\\bin\\/(true|false)' <<< "$l_loadable"; then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
        fi
    }
    module_loaded_chk()
    {
        # Check if the module is currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
    }
    module_deny_chk()
    {
        # Check if the module is deny listed
        l_dl="y"
        if modprobe --showconfig | grep -Pq -- '^h*blacklist\b+'$l_mpname'\b'; then
            l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\b\$l_mname\b" $l_searchloc)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            l_output3="$l_output3\n - \"$l_mdir\""
            [ "$l_dl" != "y" ] && module_deny_chk
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mttype" ]; then
                module_loadable_chk
                module_loaded_chk
            fi
        else
            l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
        fi
    done
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_output3" ] && echo -e "\n\n-- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
    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:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

**Remediation:**

Run the following script to disable the `rds` module:

-IF- the module is available in the running kernel:

- Create a file with `install rds /bin/false` in the `/etc/modprobe.d/` directory
- Create a file with `blacklist rds` in the `/etc/modprobe.d/` directory
- Unload `rds` from the kernel

-IF- available in ANY installed kernel:

- Create a file with `blacklist rds` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```

#!/usr/bin/env bash

{
    l_mname="rds" # set module name
    l_mtype="net" # set module type
    l_mpath="/lib/modules/**/kernel/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_fix()
    {
        # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
        #/etc/modprobe.d
        l_loadable=$(modprobe -n -v "$l_mname")
        [ $(wc -l <<< "$l_loadable") -gt "1" ] && l_loadable=$(grep -P --
        "(\^h*install\b\$l_mname\b)" <<< "$l_loadable")
        if ! grep -Pq -- '\^h*install \b/bin\b/(true|false)' <<< "$l_loadable"; then
            echo -e "\n - setting module: \"$l_mname\" to be not loadable"
            echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    module_loaded_fix()
    {
        # If the module is currently loaded, unload the module
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e "\n - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
    }
    module_deny_fix()
    {
        # If the module isn't deny listed, denylist the module
        if ! modprobe --showconfig | grep -Pq -- "\^h*blacklist\b+$l_mpname\b"; then
            echo -e "\n - deny listing \"$l_mname\""
            echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
            module_deny_fix
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
                module_loadable_fix
                module_loaded_fix
            fi
        else
            echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
        fi
    done
    echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}

```

## References:

1. NIST SP 800-53 Rev. 5: SI-4, CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

### *3.2.4 Ensure sctp kernel module is not available (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 script to verify the `sctp` module is disabled:

**-IF-** the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

**-IF-** available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

**-IF-** the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
    l_mname="sctp" # set module name
    l_mttype="net" # set module type
    l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
    l_mpath="/lib/modules/**/kernel/$l_mttype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable=$(grep -P --
"(\^h*install\b\$l_mname\b)" <<< "$l_loadable")
        if grep -Pq -- '^h*install \/bin/(true|false)' <<< "$l_loadable"; then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
        fi
    }
    module_loaded_chk()
    {
        # Check if the module is currently loaded
        if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
            l_output="$l_output\n - module: \"$l_mname\" is not loaded"
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
        fi
    }
    module_deny_chk()
    {
        # Check if the module is deny listed
        l_dl="y"
        if modprobe --showconfig | grep -Pq -- '^h*blacklist\b+'$l_mpname'\b'; then
            l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\b\$l_mname\b" $l_searchloc)\""
        else
            l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            l_output3="$l_output3\n - \"$l_mdir\""
            [ "$l_dl" != "y" ] && module_deny_chk
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mttype" ]; then
                module_loadable_chk
                module_loaded_chk
            fi
        else
            l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
        fi
    done
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_output3" ] && echo -e "\n\n-- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
    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:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

**Remediation:**

Run the following script to disable the `sctp` module:

-IF- the module is available in the running kernel:

- Create a file with `install sctp /bin/false` in the `/etc/modprobe.d/` directory
- Create a file with `blacklist sctp` in the `/etc/modprobe.d/` directory
- Unload `sctp` from the kernel

-IF- available in ANY installed kernel:

- Create a file with `blacklist sctp` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```

#!/usr/bin/env bash

{
    l_mname="sctp" # set module name
    l_mtype="net" # set module type
    l_mpath="/lib/modules/**/kernel/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")

    module_loadable_fix()
    {
        # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
        #/etc/modprobe.d
        l_loadable=$(modprobe -n -v "$l_mname")
        [ $(wc -l <<< "$l_loadable") -gt "1" ] && l_loadable=$(grep -P --
        "^(^h*install\b\$l_mname\b)" <<< "$l_loadable")
        if ! grep -Pq -- '^h*install \b/bin\//(true|false)' <<< "$l_loadable"; then
            echo -e "\n - setting module: \"$l_mname\" to be not loadable"
            echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    module_loaded_fix()
    {
        # If the module is currently loaded, unload the module
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e "\n - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
    }
    module_deny_fix()
    {
        # If the module isn't deny listed, denylist the module
        if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
            echo -e "\n - deny listing \"$l_mname\""
            echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
        fi
    }
    # Check if the module exists on the system
    for l_mdir in $l_mpath; do
        if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
            echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
            module_deny_fix
            if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
                module_loadable_fix
                module_loaded_fix
            fi
        else
            echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
        fi
    done
    echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}

```

## References:

1. NIST SP 800-53 Rev. 5: SI-4, CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

### 3.3 Configure Network Kernel Parameters

The following network parameters are intended for use on both host only and router systems. A system acts as a router if it has at least two interfaces and is configured to perform routing functions.

#### Note:

- sysctl settings are defined through files in `/usr/local/lib`, `/usr/lib/`, `/lib/`, `/run/`, and `/etc/`
- Files are typically placed in the `sysctl.d` directory within the parent directory
- 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`
- Files must have the ".conf" extension
- Vendors settings usually live in `/usr/lib/` or `/usr/local/lib/`
- 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 command `/usr/lib/systemd/systemd-sysctl --cat-config` produces output containing The system's loaded kernel parameters and the files they're configured in:
  - Entries listed latter in the file take precedence over the same settings listed earlier in the file
  - Files containing kernel parameters that are over-ridden by other files with the same name will not be listed
  - On systems running UncomplicatedFirewall, the kernel parameters may be set or over-written. This will not be visible in the output of the command
- On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`
  - The settings in `/etc/ufw/sysctl.conf` will override settings other settings and **will not** be visible in the output of the `/usr/lib/systemd/systemd-sysctl --cat-config` command
  - This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

The system's loaded kernel parameters and the files they're configured in can be viewed by running the following command:

```
# /usr/lib/systemd/systemd-sysctl --cat-config
```

### *3.3.1 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 `net.ipv4.ip_forward` and `net.ipv6.conf.all.forwarding` 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.

#### **Impact:**

IP forwarding is required on systems configured to act as a router. If these parameters are disabled, the system will not be able to perform as a router.

Many Cloud Service Provider (CSP) hosted systems require IP forwarding to be enabled. If the system is running on a CSP platform, this requirement should be reviewed before disabling IP forwarding.

#### **Audit:**

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.ip_forward` is set to 0
- `net.ipv6.conf.all.forwarding` is set to 0

#### **Note:**

- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.
- IPv6 kernel parameters only apply to systems where IPv6 is enabled

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("net.ipv4.ip_forward=0" "net.ipv6.conf.all.forwarding=0")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po '^h*([^\n\r]+|#[^\n\r\h]+\.conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="" read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// }"; l_fkpvvalue="${l_fkpvvalue// }"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\""
                fi
            done < <(grep -Po -- "^\h*$l_kpname\h*=*\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n      ** Note:\n\"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS="" read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// }"; l_kpvalue="${l_kpvalue// }"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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 "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

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

- `net.ipv4.ip_forward = 0`

### *Example:*

```
# printf '%s\n' "net.ipv4.ip_forward = 0" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

{
    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 file in `/etc/sysctl.d/` ending in `.conf`:

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

### *Example:*

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

Run the following script to set the active kernel parameters:

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

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

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## **Default Value:**

`net.ipv4.ip_forward = 0`

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

## **References:**

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## **Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

- The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf
- This behavior can be changed by updating the IPT\_SYSCTL parameter in /etc/default/ufw

## **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
T1557, T1557.000	TA0006, TA0009	M1030, M1042

### *3.3.2 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.

#### **Impact:**

IP forwarding is required on systems configured to act as a router. If these parameters are disabled, the system will not be able to perform as a router.

#### **Audit:**

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.send_redirects` is set to 0
- `net.ipv4.conf.default.send_redirects` is set to 0

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("net.ipv4.conf.all.send_redirects=0" "net.ipv4.conf.default.send_redirects=0")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' \
/etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po
'^\h*([^\n\r]+|\#\h*/[^#\n\r\h]+\.\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="" read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// }"; l_fkpvvalue="${l_fkpvvalue// }"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\""
                fi
            done < <(grep -Po -- "^\h*$l_kpname\h*=*\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n      ** Note: \"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS="" read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// }"; l_kpvalue="${l_kpvalue// }"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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:**

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

- `net.ipv4.conf.all.send_redirects = 0`
- `net.ipv4.conf.default.send_redirects = 0`

### *Example:*

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

Run the following script to set the active kernel parameters:

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

{
    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
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## **Default Value:**

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

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

## **References:**

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## **Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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 bogus icmp responses are ignored (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Setting `net.ipv4.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 script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.icmp_ignore_bogus_error_responses` is set to 1

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("net.ipv4.icmp_ignore_bogus_error_responses=1")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s* IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po '^h*([^\n\r]+|#[^\n\r\h]+\.conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS= read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// }"; l_fkpvvalue="${l_fkpvvalue// }"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\"\n"
                fi
            done < <(grep -Po -- "^\h*$l_kpname\h*=*\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n      ** Note:\n\"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS= read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// }"; l_kpvalue="${l_kpvalue// }"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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:**

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

- `net.ipv4.icmp_ignore_bogus_error_responses = 1`

### *Example:*

```
# printf '%s\n' "net.ipv4.icmp_ignore_bogus_error_responses = 1" >>
/etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

{
    sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
    sysctl -w net.ipv4.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## **Default Value:**

`net.ipv4.icmp_ignore_bogus_error_responses = 1`

## **References:**

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## **Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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
T1562, T1562.006	TA0040	M1053

### *3.3.4 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 the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.icmp_echo_ignore_broadcasts` is set to 1

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("net.ipv4.icmp_echo_ignore_broadcasts=1")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po '^h*([^\n\r]+|#[^\n\r\h]+\.conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS= read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// }"; l_fkpvvalue="${l_fkpvvalue// }"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\"\n"
                fi
            done < <(grep -Po -- "^\h*$l_kpname\h*=*\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n      ** Note:\n\"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS= read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// }"; l_kpvalue="${l_kpvalue// }"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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 "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

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

- `net.ipv4.icmp_echo_ignore_broadcasts = 1`

### *Example:*

```
# printf '%s\n' "net.ipv4.icmp_echo_ignore_broadcasts = 1" >>
/etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

{
    sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
    sysctl -w net.ipv4.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## **Default Value:**

`net.ipv4.conf.default.log_martians = 0`

## **References:**

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## **Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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	TA0040	M1037

### 3.3.5 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.

#### Rationale:

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`, `net.ipv4.conf.default.accept_redirects`,  
`net.ipv6.conf.all.accept_redirects`, and `net.ipv6.conf.default.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.

#### Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.accept_redirects` is set to 0
- `net.ipv4.conf.default.accept_redirects` is set to 0
- `net.ipv6.conf.all.accept_redirects` is set to 0
- `net.ipv6.conf.default.accept_redirects` is set to 0

#### Note:

- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.
- IPv6 kernel parameters only apply to systems where IPv6 is enabled

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("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")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s*IP_*SYSTL=/ {print $2}' /etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running
configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running
configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po
'^\h*([^\#\n\r]+|\#\h*/[^#\n\r\h]+\.\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl -
-cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS= read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// }"; l_fkpvvalue="${l_fkpvvalue// }"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvvalue\" in
\"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in
\"$(printf '%s' "${A_out[@]}")\"\n" and should have a value of: \"$l_kpvalue\"\n"
                fi
            done < <(grep -Po -- "^\h*$l_kpname\b*=*\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n    ** Note:
\"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS= read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// }"; l_kpvalue="${l_kpvalue// }"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<<
"$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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 "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

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

- net.ipv4.conf.all.accept\_redirects = 0
- net.ipv4.conf.default.accept\_redirects = 0

### *Example:*

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

Run the following script to set the active kernel parameters:

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

{
    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 file in /etc/sysctl.d/ ending in .conf:**

- net.ipv6.conf.all.accept\_redirects = 0
- net.ipv6.conf.default.accept\_redirects = 0

### *Example:*

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

Run the following script to set the active kernel parameters:

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

{
    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
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## **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
```

## **References:**

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## **Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

- The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf
- This behavior can be changed by updating the IPT\_SYSCTL parameter in /etc/default/ufw

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> 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
T1557, T1557.000	TA0006, TA0009	M1030, M1042

### 3.3.6 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` and `net.ipv4.conf.default.secure_redirects` to 0 protects the system from routing table updates by possibly compromised known gateways.

#### Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.secure_redirects` is set to 0
- `net.ipv4.conf.default.secure_redirects` is set to 0

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("net.ipv4.conf.all.secure_redirects=0" "net.ipv4.conf.default.secure_redirects=0")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po
'^\h*([^\n\r]+|\#\h*/[^#\n\r\h]+\.\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="=" read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// /}"; l_fkpvvalue="${l_fkpvvalue// /}"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\""
                fi
            done < <(grep -Po -- "^\h*$l_kpname\h*=*\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n      ** Note:\n\"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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 "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

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

- `net.ipv4.conf.all.secure_redirects = 0`
- `net.ipv4.conf.default.secure_redirects = 0`

### *Example:*

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

Run the following script to set the active kernel parameters:

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

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## **Default Value:**

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

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

## **References:**

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## **Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

### *3.3.7 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 `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` to 1 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.

#### **Impact:**

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 the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.rp_filter` is set to 1
- `net.ipv4.conf.default.rp_filter` is set to 1

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("net.ipv4.conf.all.rp_filter=1" "net.ipv4.conf.default.rp_filter=1")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' \
/etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po
'^\h*([^\n\r]+|\#\h*/[^#\n\r\h]+\.\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="=" read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// /}"; l_fkpvvalue="${l_fkpvvalue// /}"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\""
                fi
            done < <(grep -Po -- "^\h*$l_kpname\h*=*\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n      ** Note: \"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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:**

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

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

### *Example:*

```
# printf '%s\n' "net.ipv4.conf.all.rp_filter = 1"  
"net.ipv4.conf.default.rp_filter = 1" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## **Default Value:**

`net.ipv4.conf.all.rp_filter = 2`

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

## **References:**

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## **Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b></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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b></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 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 the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- net.ipv4.conf.all.accept\_source\_route **is set to 0**
- net.ipv4.conf.default.accept\_source\_route **is set to 0**
- net.ipv6.conf.all.accept\_source\_route **is set to 0**
- net.ipv6.conf.default.accept\_source\_route **is set to 0**

## Note:

- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.
- IPv6 kernel parameters only apply to systems where IPv6 is enabled

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=(`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")
    l_ufwscf="${([ -f /etc/default/ufw ] && awk -F= '/^s*IP_SYSCTL=/ {print $2}' /etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po
'^\h*([^\n\r]+|\h*/[^#\n\r\h]+\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po '^h*$l_kpname\b' "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\//.}"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="=" read -r l_fkpname l_fkpvale; do
                l_fkpname="${l_fkpname// }"; l_fkpvale="${l_fkpvale// }"
                if [ "$l_fkpvale" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvale\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvale\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\"\n"
                fi
            done < <(grep -Po -- ^h*$l_kpname\h=\h*\H+ "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n    ** Note: \"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// }"; l_kpvalue="${l_kpvalue// }"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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:**

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

- net.ipv4.conf.all.accept\_source\_route = 0
- net.ipv4.conf.default.accept\_source\_route = 0

### *Example:*

```
# printf '%s\n' "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 script to set the active kernel parameters:

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

{
    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 file in /etc/sysctl.d/ ending in .conf:**

- net.ipv6.conf.all.accept\_source\_route = 0
- net.ipv6.conf.default.accept\_source\_route = 0

### *Example:*

```
# printf '%s\n' "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:

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

{
    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
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### **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
```

### **References:**

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

### **Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in /etc/ufw/sysctl.conf

- The settings in /etc/ufw/sysctl.conf will override settings in /etc/sysctl.conf
- This behavior can be changed by updating the IPT\_SYSCTL parameter in /etc/default/ufw

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> 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
T1590, T1590.005	TA0007	

### *3.3.9 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:**

Setting `net.ipv4.conf.all.log_martians` and `net.ipv4.conf.default.log_martians` to 1 enables this feature. 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 the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.log_martians` is set to 1
- `net.ipv4.conf.default.log_martians` is set to 1

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("net.ipv4.conf.all.log_martians=1" "net.ipv4.conf.default.log_martians=1")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' \
/etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po
'^\h*([^\n\r]+|\#\h*/[^#\n\r\h]+\.\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="" read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// /}"; l_fkpvvalue="${l_fkpvvalue// /}"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\"\n"
                fi
            done < <(grep -Po -- "^\h*$l_kpname\h*=*\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n      ** Note: \"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS="" read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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 "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}

```

## **Remediation:**

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

- `net.ipv4.conf.all.log_martians = 1`
- `net.ipv4.conf.default.log_martians = 1`

### *Example:*

```
# printf '%s\n' "net.ipv4.conf.all.log_martians = 1"
# net.ipv4.conf.default.log_martians = 1" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

{
    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
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## **Default Value:**

`net.ipv4.conf.all.log_martians = 0`

`net.ipv4.conf.default.log_martians = 0`

## **References:**

1. NIST SP 800-53 Rev. 5: AU-3

## **Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.5 Collect Detailed Audit Logs</b>  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><b>6.2 Activate audit logging</b>  Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b>  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	

### *3.3.10 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. Setting `net.ipv4.tcp_syncookies` to 1 enables SYN cookies, allowing the system to keep accepting valid connections, even if under a denial of service attack.

#### **Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.tcp_syncookies` is set to 1

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("net.ipv4.tcp_syncookies=1")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po '^h*([^\n\r]+|#[^\n\r\h]+\.conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="" read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// }"; l_fkpvvalue="${l_fkpvvalue// }"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\"\n"
                fi
            done < <(grep -Po -- "^\h*$l_kpname\h*=*\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n      ** Note:\n\"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS="" read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// }"; l_kpvalue="${l_kpvalue// }"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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:**

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

- `net.ipv4.tcp_syncookies = 1`

### *Example:*

```
# printf '%s\n' "net.ipv4.tcp_syncookies = 1" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## **Default Value:**

`net.ipv4.tcp_syncookies = 1`

## **References:**

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## **Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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
T1499, T1499.001	TA0040	M1037

### *3.3.11 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. Setting `net.ipv6.conf.all.accept_ra` and `net.ipv6.conf.default.accept_ra` to 0 disables the system's ability to accept IPv6 router advertisements.

#### **Audit:**

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv6.conf.all.accept_ra` is set to 0
- `net.ipv6.conf.default.accept_ra` is set to 0

#### **Note:**

- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.
- IPv6 kernel parameters only apply to systems where IPv6 is enabled

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("net.ipv6.conf.all.accept_ra=0" "net.ipv6.conf.default.accept_ra=0")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^s*IPT_SYSCTL=/ {print $2}' \
/etc/default/ufw)"
    kernel_parameter_chk()
    {
        l_krp=$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs) # Check running configuration
        if [ "$l_krp" = "$l_kpvalue" ]; then
            l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\" in the running configuration"
        else
            l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_krp\" in the running configuration and should have a value of: \"$l_kpvalue\""
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_kpar=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
        done < <(/usr/lib/systemd/systemd-sysctl --cat-config | grep -Po
'^\h*([^\n\r]+#\h*/[^#\n\r\h]+\.\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered by systemd-sysctl --cat-config)
            l_kpar=$(grep -Po "^\h*$l_kpname\b" "$l_ufwscf" | xargs)
            l_kpar="${l_kpar//\// }"
            [ "$l_kpar" = "$l_kpname" ] && A_out+=(["$l_kpar"]="$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="=" read -r l_fkpname l_fkpvvalue; do
                l_fkpname="${l_fkpname// /}"; l_fkpvvalue="${l_fkpvvalue// /}"
                if [ "$l_fkpvvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to \"$l_fkpvvalue\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value of: \"$l_kpvalue\""
                fi
            done < <(grep -Po -- "^\h*$l_kpname\h*=*\h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_kpname\" is not set in an included file\n      ** Note: \
\"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<<
"$l_kpname"; then
            l_output="$l_output\n - IPv6 is disabled on the system, \"$l_kpname\" is not applicable"
        else
            kernel_parameter_chk
        fi
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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:**

- IF - IPv6 is enabled on the system:

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

- `net.ipv6.conf.all.accept_ra = 0`
- `net.ipv6.conf.default.accept_ra = 0`

### *Example:*

```
# printf '%s\n' "net.ipv6.conf.all.accept_ra = 0"  
"net.ipv6.conf.default.accept_ra = 0" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## **Default Value:**

`net.ipv6.conf.all.accept_ra = 1`

`net.ipv6.conf.default.accept_ra = 1`

## **References:**

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## **Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            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><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            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

## 4 Host Based Firewall

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

## 4.1 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.

### Note:

- 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.

#### *4.1.1 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-query -s ufw &>/dev/null && echo "ufw is installed"  
ufw is installed
```

##### **Remediation:**

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

```
apt install ufw
```

##### **References:**

1. NIST SP 800-53 Rev. 5: SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

## *4.1.2 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 &>/dev/null && echo "iptables-persistent is installed"
```

Nothing should be returned

### **Remediation:**

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

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

### **References:**

1. NIST SP 800-53 Rev. 5: SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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	TA0005	M1033

#### *4.1.3 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.

##### **Note:**

- 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 (e.g. 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>
2. NIST SP 800-53 Rev. 5: SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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	TA0005	M1018

#### *4.1.4 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
```

##### **References:**

1. NIST SP 800-53 Rev. 5: SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

#### *4.1.5 Ensure ufw outbound connections are configured (Manual)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Configure the firewall rules for new outbound connections.

##### **Note:**

- 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
```

##### **References:**

1. NIST SP 800-53 Rev. 5: SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

#### *4.1.6 Ensure ufw firewall rules exist for all open ports (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Services and ports can be accepted or explicitly rejected.

##### **Note:**

- 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:**

To reduce the attack surface of a system, all services and ports should be blocked unless required.

- Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.
- Without a firewall rule configured for open ports, the default firewall policy will drop all packets to these ports.
- Required ports should have a firewall rule created to allow approved connections in accordance with local site policy.
- Unapproved ports should have an explicit deny rule created.

## Audit:

Run the following script to verify a firewall rule exists for all open ports:

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

{
    unset a_ufwout;unset a_openports
    while read -r l_ufwport; do
        [ -n "$l_ufwport" ] && a_ufwout+=("$l_ufwport")
    done < <(ufw status verbose | grep -Po '^\\h*\\d+\\b' | sort -u)
    while read -r l_openport; do
        [ -n "$l_openport" ] && a_openports+=("$l_openport")
    done < <(ss -tuln | awk '$5!~/%lo:/ && $5!~/127.0.0.1:/ &&
$5!~/[::1]?:/' {split($5, a, ":"); print a[2]}' | sort -u)
    a_diff=("$({printf '%s\n' "${a_openports[@]}"} ${a_ufwout[@]}"
"${a_ufwout[@]}") | sort | uniq -u")
    if [[ -n "${a_diff[*]}" ]]; then
        echo -e "\n- Audit Result:\n  ** FAIL **\n- The following port(s) don't
have a rule in UFW: ${printf '%s\n' \\n"${a_diff[*]}"}\n- End List"
    else
        echo -e "\n- Audit Passed -\n- All open ports have a rule in UFW\n"
    fi
}
```

## Remediation:

For each port identified in the audit which does not have a firewall rule, evaluate the service listening on the port and add a rule for accepting or denying inbound connections in accordance with local site policy:

*Examples:*

```
# ufw allow in <port>/<tcp or udp protocol>

# ufw deny in <port>/<tcp or udp protocol>
```

**Note:** Examples create rules for from any, to any. More specific rules should be concentrated when allowing inbound traffic e.g only traffic from this network.

*Example to allow traffic on port 443 using the tcp protocol from the 192.168.1.0 network:*

```
ufw allow from 192.168.1.0/24 to any proto tcp port 443
```

## References:

1. NIST SP 800-53 Rev. 5: SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

#### *4.1.7 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 out http  
ufw allow out https  
ufw allow out ntp # Network Time Protocol  
ufw allow out to any port 53 # DNS  
ufw allow out to any port 853 # DNS over TLS  
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
```

## **References:**

1. NIST SP 800-53 Rev. 5: SC-7

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</b> 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

## 4.2 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 bellow as /etc/nftables.rules

```

#!/sbin/nft -f

# This nftables.rules config should be saved as /etc/nftables.rules
# flush nftables ruleset
flush ruleset
# Load nftables ruleset
# nftables config with inet table named filter
table inet filter {
    # Base chain for input hook named input (Filters inbound network
packets)
    chain input {
        type filter hook input priority 0; policy drop;

        # Ensure loopback traffic is configured
        iif "lo" accept
        ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
        ip6 saddr ::1 counter packets 0 bytes 0 drop

        # Ensure established connections are configured
        ip protocol tcp ct state established accept
        ip protocol udp ct state established accept
        ip protocol icmp ct state established accept

        # Accept port 22(SSH) traffic from anywhere
        tcp dport ssh accept

        # Accept ICMP and IGMP from anywhere
        icmpv6 type { destination-unreachable, packet-too-big, time-
exceeded, parameter-problem, mld-listener-query, mld-listener-report, mld-
listener-done, nd-router-solicit, nd-router-advert, nd-neighbor-solicit, nd-
neighbor-advert, ind-neighbor-solicit, ind-neighbor-advert, mld2-listener-
report } accept
        icmp type { destination-unreachable, router-advertisement,
router-solicitation, time-exceeded, parameter-problem } accept
        ip protocol igmp accept
    }

    # Base chain for hook forward named forward (Filters forwarded
network packets)
    chain forward {
        type filter hook forward priority 0; policy drop;
    }

    # Base chain for hook output named output (Filters outbound network
packets)
    chain output {
        type filter hook output priority 0; policy drop;
        # Ensure outbound and established connections are configured
        ip protocol tcp ct state established,related,new accept
        ip protocol udp ct state established,related,new accept
        ip protocol icmp ct state established,related,new accept
    }
}

```

Run the following command to load the file into nftables

```
# nft -f /etc/nftables.rules
```

All changes in the nftables subsections are temporary.

To make these changes permanent:

Run the following command to create the nftables.rules file

```
nft list ruleset > /etc/nftables.rules
```

Add the following line to /etc/nftables.conf

```
include "/etc/nftables.rules"
```

#### *4.2.1 Ensure nftables is installed (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

nftables provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM) and a new nft userspace command line tool. nftables reuses the existing Netfilter subsystems such as the existing hook infrastructure, the connection tracking system, NAT, userspace queuing and logging subsystem.

##### **Notes:**

- nftables is available in Linux kernel 3.13 and newer
- Only one firewall utility should be installed and configured
- Changing firewall settings while connected over the network can result in being locked out of the system

##### **Rationale:**

nftables is a subsystem of the Linux kernel that can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

##### **Audit:**

Run the following command to verify that nftables is installed:

```
# dpkg-query -s nftables &>/dev/null && echo "nftables is installed"  
nftables is installed
```

##### **Remediation:**

Run the following command to install nftables:

```
# apt install nftables
```

##### **References:**

1. NIST SP 800-53 Rev. 5: CA-9

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

## 4.2.2 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 &>/dev/null && echo "ufw is installed"
```

Nothing should be returned

-OR-

Run the following commands to verify `ufw` is disabled and `ufw.service` is not enabled:

```
# ufw status  
Status: inactive  
# systemctl is-enabled ufw.service  
masked
```

### Remediation:

Run **one** of the following to either remove `ufw` or disable `ufw` and mask `ufw.service`:

Run the following command to remove `ufw`:

```
# apt purge ufw
```

-OR-

Run the following commands to disable `ufw` and mask `ufw.service`:

```
# ufw disable  
# systemctl stop ufw.service  
# systemctl mask ufw.service
```

**Note:** `ufw disable` needs to be run before `systemctl mask ufw.service` in order to correctly disable UFW

## References:

1. NIST SP 800-53 Rev. 5: SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b> 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	TA0005	M1033

#### *4.2.3 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
```

##### **References:**

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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	TA0005	

#### *4.2.4 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 built, 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
```

##### **References:**

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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	M1047

#### *4.2.5 Ensure nftables base chains exist (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

##### **Rationale:**

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

##### **Impact:**

If configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

##### **Audit:**

Run the following commands and verify that base chains exist for INPUT.

```
# nft list ruleset | grep 'hook input'  
type filter hook input priority 0;
```

Run the following commands and verify that base chains exist for FORWARD.

```
# nft list ruleset | grep 'hook forward'  
type filter hook forward priority 0;
```

Run the following commands and verify that base chains exist for OUTPUT.

```
# nft list ruleset | grep 'hook output'  
type filter hook output priority 0;
```

## Remediation:

Run the following command to create the base chains:

```
# nft create chain inet <table name> <base chain name> { type filter hook <(input|forward|output)> priority 0 \; }
```

*Example:*

```
# nft create chain inet filter input { type filter hook input priority 0 \; }

# nft create chain inet filter forward { type filter hook forward priority 0 \; }

# nft create chain inet filter output { type filter hook output priority 0 \; }
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</b> 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	M1047

## 4.2.6 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 the 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:

Run the following command to verify the loopback interface is configured to accept network traffic:

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'iif "lo" accept'
```

#### Example output:

```
iif "lo" accept
```

Run the following command to verify network traffic from an IPv4 loopback interface is configured to drop:

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'ip saddr'
```

#### Example output:

```
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 network traffic from an IPv6 loopback interface is configured to drop:

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'ip6 saddr'
```

#### Example output:

```
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
```

## **References:**

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</b> 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	

## *4.2.7 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
```

## **References:**

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1562	TA0011	M1031, M1037

## 4.2.8 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
2. NIST SP 800-53 Rev. 5: CA-9, SC-7

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1562, T1562.004	TA0011	M1031, M1037

#### *4.2.9 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
```

##### **References:**

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

#### *4.2.10 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"
```

## **References:**

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</b> 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

## 4.3 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

### **4.3.1 Configure iptables software**

This section provides guidance for installing, enabling, removing, and disabling software packages necessary for using IPTTables 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 Uncomplicated Firewall (UFW) or NFTables are being used for configuration and maintenance, this section should be skipped and the guidance in their respective section followed.

#### *4.3.1.1 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` is installed:

```
# dpkg-query -s iptables &>/dev/null && echo "iptables is installed"  
iptables is installed
```

Run the following command to verify that `iptables-persistent` is installed:

```
# dpkg-query -s iptables-persistent &>/dev/null && echo "iptables-persistent  
is installed"  
iptables-persistent is installed
```

##### **Remediation:**

Run the following command to install `iptables` and `iptables-persistent`

```
# apt install iptables iptables-persistent
```

##### **References:**

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

#### *4.3.1.2 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-query -s nftables &>/dev/null && echo "nftables is installed"  
nftables is installed
```

##### **Remediation:**

Run the following command to remove `nftables`:

```
# apt purge nftables
```

##### **References:**

1. NIST SP 800-53 Rev. 5: CA-9, CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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	

#### *4.3.1.3 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 &>/dev/null && echo "ufw is installed"
```

Nothing should be returned.

**- OR -**

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  
# systemctl stop ufw  
# systemctl mask ufw
```

**Note:** `ufw disable` needs to be run before `systemctl mask ufw` in order to correctly disable UFW

## References:

1. NIST SP 800-53 Rev. 5: CA-9, CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</b> 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	

### 4.3.2 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
```

#### *4.3.2.1 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
```

##### **References:**

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

#### 4.3.2.2 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 the 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
```

## References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</b> 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

#### *4.3.2.3 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
```

##### **References:**

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

#### *4.3.2.4 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
```

## References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

### 4.3.3 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
```

#### *4.3.3.1 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 enabled on the system.

```
#!/usr/bin/bash

{
    if grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable; then
        echo -e "- IPv6 is enabled on the system"
    else
        echo -e "- IPv6 is not enabled on the system"
    fi
}
```

## Remediation:

IF IPv6 is enabled on your system:

Run the following commands to implement a default DROP policy:

```
# ip6tables -P INPUT DROP
# ip6tables -P OUTPUT DROP
# ip6tables -P FORWARD DROP
```

## References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

#### *4.3.3.2 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 enabled on the system.

```
#!/usr/bin/bash

{
    if grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable; then
        echo -e "- IPv6 is enabled on the system"
    else
        echo -e "- IPv6 is not enabled on the system"
    fi
}
```

## 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
```

## References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

#### *4.3.3.3 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 enabled on the system.

```
#!/usr/bin/bash

{
    if grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable; then
        echo -e "- IPv6 is enabled on the system"
    else
        echo -e "- IPv6 is not enabled on the system"
    fi
}
```

## **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
```

## **References:**

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</b> 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

#### *4.3.3.4 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
```

## References:

1. NIST SP 800-53 Rev. 5: CA-9, SC-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>4.5 Implement and Manage a Firewall on End-User Devices</b>            Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b>            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

## **5 Access Control**

## 5.1 Configure SSH Server

Secure Shell (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.**
- The openSSH daemon configuration directives, `Include` and `Match`, may cause the audits in this section's recommendations to report incorrectly. It is recommended that these options only be used if they're needed and fully understood. If these options are configured in accordance with local site policy, they should be accounted for when following the recommendations in this section.
- The default `Include` location is the `/etc/ssh/sshd_config.d` directory. This default has been accounted for in this section. If a file has an additional `Include` that isn't this default location, the files should be reviewed to verify that the recommended setting is not being over-ridden.
- The audits of the running configuration in this section are run in the context of the root user, the local host name, and the local host's IP address. If a `Match` block exists that matches one of these criteria, the output of the audit will be from the match block. The respective matched criteria should be replaced with a non-matching substitution.
- `Include`:
  - `Include` the specified configuration file(s).
  - Multiple pathnames may be specified and each pathname may contain `glob(7)` wildcards that will be expanded and processed in lexical order.
  - Files without absolute paths are assumed to be in `/etc/ssh/`.
  - An `Include` directive may appear inside a `Match` block to perform conditional inclusion.

- Match:
  - Introduces a conditional block. If all of the criteria on the Match line are satisfied, the keywords on the following lines override those set in the global section of the config file, until either another Match line or the end of the file. If a keyword appears in multiple Match blocks that are satisfied, only the first instance of the keyword is applied.
  - The arguments to Match are one or more criteria-pattern pairs or the single token All which matches all criteria. The available criteria are User, Group, Host, LocalAddress, LocalPort, and Address.
  - The match patterns may consist of single entries or comma-separated lists and may use the wildcard and negation operators described in the PATTERNS section of ssh\_config(5).
  - The patterns in an Address criteria may additionally contain addresses to match in CIDR address/masklen format, such as 192.0.2.0/24 or 2001:db8::/32. Note that the mask length provided must be consistent with the address - it is an error to specify a mask length that is too long for the address or one with bits set in this host portion of the address. For example, 192.0.2.0/33 and 192.0.2.0/8, respectively.
  - Only a subset of keywords may be used on the lines following a Match keyword. Available keywords are available in the ssh\_config man page.
- Once all configuration changes have been made to /etc/ssh/sshd\_config or any included configuration files, the sshd configuration must be reloaded

Command to re-load the SSH daemon configuration:

```
# systemctl reload-or-restart sshd
```

### *5.1.1 Ensure permissions on /etc/ssh/sshd\_config are configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The file `/etc/ssh/sshd_config`, and files ending in `.conf` in the `/etc/ssh` directory, contain configuration specifications for `sshd`.

#### **Rationale:**

configuration specifications for `sshd` need to be protected from unauthorized changes by non-privileged users.

## Audit:

Run the following script and verify `/etc/ssh/sshd_config` and files ending in `.conf` in the `/etc/ssh/sshd_config.d` directory are:

- Mode 0600 or more restrictive
- Owned by the root user
- Group owned by the group root.

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

{
    l_output="" l_output2=""
    perm_mask='0177' && maxperm=$( printf '%o' $(( 0777 & ~$perm_mask)) )
    SSHD_FILES_CHK()
    {
        while IFS=: read -r l_mode l_user l_group; do
            l_out2=""
            [ $(($l_mode & $perm_mask)) -gt 0 ] && l_out2="$l_out2\n - Is mode: \"$l_mode\" should be: \"$maxperm\" or more restrictive"
            [ "$l_user" != "root" ] && l_out2="$l_out2\n - Is owned by \"$l_user\" should be owned by \"root\""
            [ "$l_group" != "root" ] && l_out2="$l_out2\n - Is group owned by \"$l_user\" should be group owned by \"root\""
            if [ -n "$l_out2" ]; then
                l_output2="$l_output2\n - File: \"$l_file\":$l_out2"
            else
                l_output="$l_output\n - File: \"$l_file\":\n - Correct: mode ($l_mode), owner ($l_user), and group owner ($l_group) configured"
            fi
            done < <(stat -Lc '%#a:%U:%G' "$l_file")
        }
        [ -e "/etc/ssh/sshd_config" ] && l_file="/etc/ssh/sshd_config" &&
        SSHD_FILES_CHK
        while IFS= read -r -d $'\0' l_file; do
            [ -e "$l_file" ] && SSHD_FILES_CHK
            done < <(find -L /etc/ssh/sshd_config.d -type f  \(\ -perm /077 -o ! -user root -o ! -group root \) -print0 2>/dev/null)
            if [ -z "$l_output2" ]; then
                echo -e "\n- Audit Result:\n *** PASS ***\n- * Correctly set *\n:$l_output\n"
            else
                echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit failure *\n:$l_output2\n"
                [ -n "$l_output" ] && echo -e " - * Correctly set *\n:$l_output\n"
            fi
    }
}
```

- IF - other locations are listed in an `Include` statement, \*.conf files in these locations should also be checked.

## Remediation:

Run the following script to set ownership and permissions on `/etc/ssh/sshd_config` and files ending in `.conf` in the `/etc/ssh/sshd_config.d` directory:

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

{
    chmod u-x,og-rwx /etc/ssh/sshd_config
    chown root:root /etc/ssh/sshd_config
    while IFS= read -r -d $'\0' l_file; do
        if [ -e "$l_file" ]; then
            chmod u-x,og-rwx "$l_file"
            chown root:root "$l_file"
        fi
    done < <(find /etc/ssh/sshd_config.d -type f -print0 2>/dev/null)
}
```

- IF - other locations are listed in an `Include` statement, `*.conf` files in these locations access should also be modified.

## References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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
T1098, T1098.004, T1543, T1543.002	TA0005	M1022

## *5.1.2 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 owned by the root user and either:

- owned by the group root and mode 0600 or more restrictive

**- OR -**

- owned by the group designated to own openSSH private keys and mode 0640 or more restrictive

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    l_ssh_group_name=$(awk -F: '$(1 ~ /^(ssh_keys|_?ssh)$) {print $1}' /etc/group)
    FILE_CHK()
    {
        while IFS=: read -r l_file_mode l_file_owner l_file_group; do
            l_out2=""
            [ "$l_file_group" = "$l_ssh_group_name" ] && l_pmask="0137" ||
            l_pmask="0177"
            l_maxperm=$( printf '%o' $(( 0777 & ~$l_pmask )) )
            if [ $(($l_file_mode & $l_pmask)) -gt 0 ]; then
                l_out2="$l_out2\n - Mode: \"$l_file_mode\" should be mode:
\"$l_maxperm\" or more restrictive"
            fi
            if [ "$l_file_owner" != "root" ]; then
                l_out2="$l_out2\n - Owned by: \"$l_file_owner\" should be owned
by \"root\""
            fi
            if [[ ! "$l_file_group" =~ ($l_ssh_group_name|root) ]]; then
                l_out2="$l_out2\n - Owned by group \"$l_file_group\" should be
group owned by: \"$l_ssh_group_name\" or \"root\""
            fi
            if [ -n "$l_out2" ]; then
                l_output2="$l_output2\n - File: \"$l_file\"$l_out2"
            else
                l_output="$l_output\n - File: \"$l_file\"\n - Correct: mode:
\"$l_file_mode\", owner: \"$l_file_owner\", and group owner:
\"$l_file_group\" configured"
            fi
            done <<(stat -Lc '%#a:%U:%G' "$l_file")
        }
        while IFS= read -r -d $'\0' l_file; do
            if ssh-keygen -lf &>/dev/null "$l_file"; then
                file "$l_file" | grep -Piq --
'\bopenssh\b+[^\#\n\r]+\h+)?private\h+key\b' && FILE_CHK
            fi
            done <<(find -L /etc/ssh -xdev -type f -print0 2>/dev/null)
            if [ -z "$l_output2" ]; then
                [ -z "$l_output" ] && l_output="\n - No openSSH private keys found"
                echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured *
:$l_output"
            else
                echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :$l_output2\n"
                [ -n "$l_output" ] && echo -e "\n - * Correctly configured *
:$n$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_output="" l_output2=""
    l_ssh_group_name=$(awk -F: '$(1 ~ /^(ssh_keys|_?ssh)$) {print $1}' /etc/group)
    FILE_ACCESS_FIX()
    {
        while IFS=: read -r l_file_mode l_file_owner l_file_group; do
            echo "File: \"$l_file\" mode: \"$l_file_mode\" owner \"$l_file_owner\" group \"$l_file_group\""
            l_out2=""
            [ "$l_file_group" = "$l_ssh_group_name" ] && l_pmask="0137" ||
            l_pmask="0177"
            l_maxperm=$( printf '%o' $(( 0777 & ~$l_pmask )) )
            if [ $(( $l_file_mode & $l_pmask )) -gt 0 ]; then
                l_out2="$l_out2\n - Mode: \"$l_file_mode\" should be mode: \"$l_maxperm\" or more restrictive\n - updating to mode: \:$l_maxperm"
                [ "$l_file_group" = "$l_ssh_group_name" ] && chmod u-x,g-wx,o-rwx "$l_file" ||
                chmod u-x,go-rwx
            fi
            if [ "$l_file_owner" != "root" ]; then
                l_out2="$l_out2\n - Owned by: \"$l_file_owner\" should be owned by \"root\"\n - Changing ownership to \"root\""
                chown root "$l_file"
            fi
            if [[ ! "$l_file_group" =~ ($l_ssh_group_name|root) ]]; then
                [ -n "$l_ssh_group_name" ] && l_new_group="$l_ssh_group_name" ||
                l_new_group="root"
                l_out2="$l_out2\n - Owned by group \"$l_file_group\" should be group owned by: \"$l_ssh_group_name\" or \"root\"\n - Changing group ownership to \"$l_new_group\""
                chgrp "$l_new_group" "$l_file"
            fi
            if [ -n "$l_out2" ]; then
                l_output2="$l_output2\n - File: \"$l_file\"$l_out2"
            else
                l_output="$l_output\n - File: \"$l_file\"\n - Correct: mode: \"$l_file_mode\", owner: \"$l_file_owner\", and group owner: \"$l_file_group\" configured"
            fi
            done < <(stat -Lc '%#a:%U:%G' "$l_file")
        }
        while IFS= read -r -d $'\0' l_file; do
            if ssh-keygen -lf &>/dev/null "$l_file"; then
                file "$l_file" | grep -Piq --
        '\bopenssh\b+([^\#\n\r]+\bprivate\b)' && FILE_ACCESS_FIX
            fi
            done < <(find -L /etc/ssh -xdev -type f -print0 2>/dev/null)
            if [ -z "$l_output2" ]; then
                echo -e "\n- No access changes required\n"
            else
                echo -e "\n- Remediation results:\n$l_output2\n"
            fi
    }
}

```

**References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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
T1552, T1552.004	TA0003, TA0006	M1022

### *5.1.3 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:

Run the following script to verify SSH public host key files are mode 0644 or more restrictive, owned by the root user, and owned by the root group:

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

{
    l_output="" l_output2=""
    l_pmask="0133" && l_maxperm=$(( printf '%o' $(( 0777 & ~$l_pmask )) ))
FILE_CHK()
{
    while IFS=: read -r l_file_mode l_file_owner l_file_group; do
        l_out2=""
        if [ $(( l_file_mode & $l_pmask )) -gt 0 ]; then
            l_out2="$l_out2\n - Mode: \"$l_file_mode\" should be mode:
\"$l_maxperm\" or more restrictive"
        fi
        if [ "$l_file_owner" != "root" ]; then
            l_out2="$l_out2\n - Owned by: \"$l_file_owner\" should be owned
by \"root\""
        fi
        if [ "$l_file_group" != "root" ]; then
            l_out2="$l_out2\n - Owned by group \"$l_file_group\" should be
group owned by group: \"root\""
        fi
        if [ -n "$l_out2" ]; then
            l_output2="$l_output2\n - File: \"$l_file\"$l_out2"
        else
            l_output="$l_output\n - File: \"$l_file\"\n - Correct: mode:
\"$l_file_mode\", owner: \"$l_file_owner\", and group owner:
\"$l_file_group\" configured"
        fi
        done < <(stat -Lc '%#a:%U:%G' "$l_file")
    }
    while IFS= read -r -d $'\0' l_file; do
        if ssh-keygen -lf &>/dev/null "$l_file"; then
            file "$l_file" | grep -Piq --
    '\bopenssh\b+h+([^\#\n\r]+\h+)?public\h+key\b' && FILE_CHK
        fi
    done < <(find -L /etc/ssh -xdev -type f -print0 2>/dev/null)
    if [ -z "$l_output2" ]; then
        [ -z "$l_output" ] && l_output="\n - No openSSH public keys found"
        echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured *\n:$l_output"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure *\n:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n - * Correctly configured *\n:$l_output\n"
    fi
}
```

## **Remediation:**

Run the following script to set mode, ownership, and group on the public SSH host key files:

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

{
    l_output="" l_output2=""
    l_pmask="0133" && l_maxperm=$(( printf '%o' $(( 0777 & ~$l_pmask )) ))
FILE_ACCESS_FIX()
{
    while IFS=: read -r l_file_mode l_file_owner l_file_group; do
        l_out2=""
        if [ $(( $l_file_mode & $l_pmask )) -gt 0 ]; then
            l_out2="$l_out2\n - Mode: \"$l_file_mode\" should be mode:
\"$l_maxperm\" or more restrictive\n - updating to mode: \:$l_maxperm\""
            chmod u-x,go-wx
        fi
        if [ "$l_file_owner" != "root" ]; then
            l_out2="$l_out2\n - Owned by: \"$l_file_owner\" should be owned
by \"root\"\n - Changing ownership to \"root\""
            chown root "$l_file"
        fi
        if [ "$l_file_group" != "root" ]; then
            l_out2="$l_out2\n - Owned by group \"$l_file_group\" should be
group owned by: \"root\"\n - Changing group ownership to \"root\""
            chgrp root "$l_file"
        fi
        if [ -n "$l_out2" ]; then
            l_output2="$l_output2\n - File: \"$l_file\"$l_out2"
        else
            l_output="$l_output\n - File: \"$l_file\"\n - Correct: mode:
\"$l_file_mode\", owner: \"$l_file_owner\", and group owner:
\"$l_file_group\" configured"
        fi
        done < <(stat -Lc '%#a:%U:%G' "$l_file")
    }
    while IFS= read -r -d $'\0' l_file; do
        if ssh-keygen -lf &>/dev/null "$l_file"; then
            file "$l_file" | grep -Piq --
    '\bopenssh\b+([^\#\n\r]+\bpublic\b) ?public\b+key\b' && FILE_ACCESS_FIX
        fi
    done < <(find -L /etc/ssh -xdev -type f -print0 2>/dev/null)
    if [ -z "$l_output2" ]; then
        echo -e "\n- No access changes required\n"
    else
        echo -e "\n- Remediation results:\n$l_output2\n"
    fi
}
```

## **Default Value:**

644 0/root 0/root

**References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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
T1557, T1557.000	TA0003, TA0006	M1022

## *5.1.4 Ensure sshd access is configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

- AllowUsers:
  - The `AllowUsers` variable gives the system administrator the option of allowing specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of `user@host`.
- AllowGroups:
  - The `AllowGroups` variable gives the system administrator the option of allowing specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.
- DenyUsers:
  - The `DenyUsers` variable gives the system administrator the option of denying specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of `user@host`.
- DenyGroups:
  - The `DenyGroups` variable gives the system administrator the option of denying specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

### **Rationale:**

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

## Audit:

Run the following command and verify the output:

```
# sshd -T | grep -Pi -- '^\\h*(allow|deny) (users|groups) \\h+\\H+'
```

Verify that the output matches at least one of the following lines:

```
allowusers <userlist>
-OR-
allowgroups <grouplist>
-OR-
denyusers <userlist>
-OR-
denygroups <grouplist>
```

Review the list(s) to ensure included users and/or groups follow local site policy

- IF - Match set statements are used in your environment, specify the connection parameters to use for the -T extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user sshuser:*

```
# sshd -T -C user=sshuser | grep -Pi --
'^\\h*(allow|deny) (users|groups) \\h+\\H+'
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple -C options or as a comma-separated list. The keywords are `addr` (source address), `user` (user), `host` (resolved source host name), `laddr` (local address), `lport` (local port number), and `rdomain` (routing domain).

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set one or more of the parameters above any `Include` and `Match` set statements as follows:

```
AllowUsers <userlist>
- AND/OR -
AllowGroups <grouplist>
```

## Note:

- First occurrence of a option takes precedence, `Match` set statements notwithstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a `.conf` file in a `Include` directory.
- It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user or group and forget to add it to the deny list.

## Default Value:

None

## References:

1. SSHD\_CONFIG(5)
2. SSHD(8)
3. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>4.3 Ensure the Use of Dedicated Administrative Accounts</b> 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.	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021, T1021.004	TA0008	M1018

## 5.1.5 Ensure sshd 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 to verify `Banner` is set:

```
# sshd -T | grep -Pi -- '^banner\h+\/\H+'
```

### Example:

```
banner /etc/issue.net
```

- IF - `Match` set statements are used in your environment, specify the connection parameters to use for the `-T` extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user `sshuser`:*

```
# sshd -T -C user=sshuser | grep -Pi -- '^banner\h+\/\H+'
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple `-C` options or as a comma-separated list. The keywords are `addr` (source address), `user` (user), `host` (resolved source host name), `laddr` (local address), `lport` (local port number), and `rdomain` (routing domain).

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `Banner` parameter above any `Include` and `Match` entries as follows:

```
Banner /etc/issue.net
```

**Note:** First occurrence of a option takes precedence, Match set statements notwithstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

**References:**

1. SSHD(8)
2. SSHD\_CONFIG(5)
3. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
	TA0001, TA0007	M1035

## *5.1.6 Ensure sshd Ciphers are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

This variable limits the ciphers that SSH can use during communication.

### **Notes:**

- 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 compliant are:
  - [aes256-gcm@openssh.com](#)
  - [aes128-gcm@openssh.com](#)
  - aes256-ctr
  - aes192-ctr
  - aes128-ctr

### **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 to verify none of the "weak" ciphers are being used:

```
# sshd -T | grep -Pi --  
'^ciphers\b+\"?([^\#\n\r]+,)?\((3des|blowfish|cast128|aes(128|192|256)|cbc|arcfour(128|256)|rijndael-cbc@lysator.liu.se|chacha20-poly1305@openssh.com)\b'
```

- IF - a line is returned, review the list of ciphers. If the line includes chacha20-poly1305@openssh.com, review CVE-2023-48795 and verify the system has been patched. No ciphers in the list below should be returned as they're considered "weak":

```
3des-cbc  
aes128-cbc  
aes192-cbc  
aes256-cbc
```

## Remediation:

Edit the /etc/ssh/sshd\_config file and add/modify the Ciphers line to contain a comma separated list of the site unapproved (weak) Ciphers preceded with a - above any Include entries:

*Example:*

```
Ciphers -3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,chacha20-poly1305@openssh.com
```

- IF - CVE-2023-48795 has been addressed, and it meets local site policy, chacha20-poly1305@openssh.com may be removed from the list of excluded ciphers.

**Note:** First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

## Default Value:

Ciphers [chacha20-poly1305@openssh.com](#),[aes128-ctr](#),[aes192-ctr](#),[aes256-ctr](#),[aes128-gcm@openssh.com](#),[aes256-gcm@openssh.com](#)

## References:

1. <https://nvd.nist.gov/vuln/detail/CVE-2023-48795>
2. <https://nvd.nist.gov/vuln/detail/CVE-2019-1543>
3. <https://nvd.nist.gov/vuln/detail/CVE-2016-2183>
4. <https://nvd.nist.gov/vuln/detail/CVE-2008-5161>
5. <https://www.openssh.com/txt/cbc.adv>
6. <https://www.openssh.com/txt/cbc.adv>
7. SSHD\_CONFIG(5)
8. SSHD(8)
9. NIST SP 800-53 Rev. 5: SC-8

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 Encrypt Sensitive Data in Transit</b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 Encrypt All Sensitive Information in Transit</b> Encrypt all sensitive information in transit.		●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1557	TA0006	M1041

## *5.1.7 Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

**Note:** To clarify, the two settings described below are only meant for idle connections from a protocol perspective and are 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 command and verify `ClientAliveInterval` and `ClientAliveCountMax` are greater than zero:

```
# sshd -T | grep -Pi -- '(clientaliveinterval|clientalivecountmax)'
```

### Example Output:

```
clientaliveinterval 15  
clientalivecountmax 3
```

- IF - Match set statements are used in your environment, specify the connection parameters to use for the `-T` extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user `sshuser`:*

```
# sshd -T -C user=sshuser | grep -Pi --  
'(clientaliveinterval|clientalivecountmax)'
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple `-C` options or as a comma-separated list. The keywords are `addr` (source address), `user` (user), `host` (resolved source host name), `laddr` (local address), `lport` (local port number), and `rdomain` (routing domain).

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `ClientAliveInterval` and `ClientAliveCountMax` parameters above any `Include` and `Match` entries according to site policy.

### Example:

```
ClientAliveInterval 15  
ClientAliveCountMax 3
```

**Note:** First occurrence of a option takes precedence, Match set statements notwithstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

**Default Value:**

ClientAliveInterval 0

ClientAliveCountMax 3

**References:**

1. SSHD\_CONFIG(5)
2. SSHD(8)
3. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**Additional Information:**

[https://bugzilla.redhat.com/show\\_bug.cgi?id=1873547](https://bugzilla.redhat.com/show_bug.cgi?id=1873547)

[https://github.com/openssh/openssh-portable/blob/V\\_8\\_9/serverloop.c#L137](https://github.com/openssh/openssh-portable/blob/V_8_9/serverloop.c#L137)

**MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003	TA0001	M1026

## *5.1.8 Ensure sshd DisableForwarding is enabled (Automated)*

### **Profile Applicability:**

- Level 1 - Workstation
- Level 2 - Server

### **Description:**

The `DisableForwarding` parameter disables all forwarding features, including X11, `ssh-agent(1)`, TCP and StreamLocal. This option overrides all other forwarding-related options and may simplify restricted configurations.

- X11Forwarding provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.
- `ssh-agent` is a program to hold private keys used for public key authentication. Through use of environment variables the agent can be located and automatically used for authentication when logging in to other machines using `ssh`.
- 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:**

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.

anyone with root privilege on the the intermediate server can make free use of `ssh-agent` to authenticate them to other servers

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 to verify `DisableForwarding` is set to yes:

```
# sshd -T | grep -i disableforwarding  
disableforwarding yes
```

## **Remediation:**

Edit the `/etc/ssh/sshd_config` file to set the `DisableForwarding` parameter to yes above any `Include` entry as follows:

```
DisableForwarding yes
```

**Note:** First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

## **References:**

1. `sshd_config(5)`
2. `SSHD(8)`
3. NIST SP 800-53 Rev. 5: CM-7

## **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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1210, T1210.000	TA0008	M1042

## 5.1.9 Ensure sshd GSSAPIAuthentication is disabled (Automated)

### Profile Applicability:

- Level 1 - Workstation
- Level 2 - Server

### Description:

The `GSSAPIAuthentication` parameter specifies whether user authentication based on GSSAPI is allowed

### Rationale:

Allowing GSSAPI authentication through SSH exposes the system's GSSAPI to remote hosts, and should be disabled to reduce the attack surface of the system

### Audit:

Run the following command to verify `GSSAPIAuthentication` is set to `no`:

```
# sshd -T | grep gssapiauthentication  
gssapiauthentication no
```

- IF `Match` set statements are used in your environment, specify the connection parameters to use for the `-T` extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user `sshuser`:*

```
# sshd -T -C user=sshuser | grep gssapiauthentication
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple `-C` options or as a comma-separated list. The keywords are `addr` (source address), `user` (user), `host` (resolved source host name), `laddr` (local address), `lport` (local port number), and `rdomain` (routing domain)

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `GSSAPIAuthentication` parameter to `no` above any `Include` and `Match` entries as follows:

```
GSSAPIAuthentication no
```

**Note:** First occurrence of an option takes precedence, `Match` set statements notwithstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

**Default Value:**

GSSAPIAuthentication no

**References:**

1. SSHD\_CONFIG(5)
2. SSHD(8)
3. 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><b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.</p>	●	●	●
v7	<p><b>4.4 Use Unique Passwords</b> 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>		●	●

**MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0001	M1042

## 5.1.10 Ensure sshd 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 to verify `HostbasedAuthentication` is set to no:

```
# sshd -T | grep hostbasedauthentication  
hostbasedauthentication no
```

- IF - Match set statements are used in your environment, specify the connection parameters to use for the `-T` extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user `sshuser`:*

```
# sshd -T -C user=sshuser | grep hostbasedauthentication
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple `-C` options or as a comma-separated list. The keywords are `addr` (source address), `user` (user), `host` (resolved source host name), `laddr` (local address), `lport` (local port number), and `rdomain` (routing domain)

## **Remediation:**

Edit the `/etc/ssh/sshd_config` file to set the `HostbasedAuthentication` parameter to `no` above any `Include` and `Match` entries as follows:

```
HostbasedAuthentication no
```

**Note:** First occurrence of a option takes precedence, `Match` set statements notwithstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

## **Default Value:**

`HostbasedAuthentication no`

## **References:**

1. [SSHD\\_CONFIG\(5\)](#)
2. [SSHD\(8\)](#)
3. [NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5](#)

## **MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0001	M1042

## 5.1.11 Ensure sshd 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 to verify `IgnoreRhosts` is set to `yes`:

```
# sshd -T | grep ignorerhosts  
ignorerhosts yes
```

- IF - Match set statements are used in your environment, specify the connection parameters to use for the `-T` extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user `sshuser`:*

```
# sshd -T -C user=sshuser | grep ignorerhosts
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple `-C` options or as a comma-separated list. The keywords are `addr` (source address), `user` (user), `host` (resolved source host name), `laddr` (local address), `lport` (local port number), and `rdomain` (routing domain)

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `IgnoreRhosts` parameter to `yes` above any `Include` and `Match` entries as follows:

```
IgnoreRhosts yes
```

**Note:** First occurrence of a option takes precedence, `Match` set statements notwithstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

### Default Value:

`IgnoreRhosts yes`

## References:

1. SSHD\_CONFIG(5)
2. SSHD(8)
3. 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	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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	TA0001	M1027

## *5.1.12 Ensure sshd KexAlgorithms is configured (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 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

### **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 to verify none of the "weak" Key Exchange algorithms are being used:

```
# sshd -T | grep -Pi -- 'kexalgorithms\h+([^\#\n\r]+,)?(diffie-hellman-group1-sha1|diffie-hellman-group14-sha1|diffie-hellman-group-exchange-sha1)\b'
```

Nothing should be returned

The following are considered "weak" Key Exchange Algorithms, and should not be used:

```
diffie-hellman-group1-sha1  
diffie-hellman-group14-sha1  
diffie-hellman-group-exchange-sha1
```

## Remediation:

Edit the `/etc/ssh/sshd_config` file and add/modify the `KexAlgorithms` line to contain a comma separated list of the site unapproved (weak) KexAlgorithms preceded with a `-` above any `Include` entries:

*Example:*

```
KexAlgorithms -diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1
```

**Note:** First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

## Default Value:

KexAlgorithms [sntrup761x25519-sha512@openssh.com](mailto:sntrup761x25519-sha512@openssh.com),curve25519-sha256,[curve25519-sha256@libssh.org](mailto:curve25519-sha256@libssh.org),ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256

## References:

1. <https://ubuntu.com/server/docs/openssh-crypto-configuration>
2. NIST SP 800-53 Rev. 5: SC-8
3. SSHD(8)
4. SSHD\_CONFIG(5)

## **Additional Information:**

The supported algorithms 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
```

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 Encrypt Sensitive Data in Transit</b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 Encrypt All Sensitive Information in Transit</b> Encrypt all sensitive information in transit.		●	●

## **MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1557, T1557.000	TA0006	M1041

### *5.1.13 Ensure sshd LoginGraceTime is configured (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:

```
# sshd -T | grep logingracetime  
logingracetime 60
```

#### **Remediation:**

Edit the `/etc/ssh/sshd_config` file to set the `LoginGraceTime` parameter to 60 seconds or less above any `Include` entry as follows:

```
LoginGraceTime 60
```

**Note:** First occurrence of a option takes precedence. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

#### **Default Value:**

`LoginGraceTime 120`

**References:**

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-6
3. SSHD(8)

**MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.003, T1110.004	TA0006	M1036

## 5.1.14 Ensure sshd LogLevel is configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

SSH provides several logging levels with varying amounts of verbosity. The `DEBUG` options are specifically not recommended other than strictly for debugging SSH communications. These levels provide so much data that it is difficult to identify important security information, and may violate the privacy of users.

### Rationale:

The `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.

The `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.

### Audit:

Run the following command and verify that output matches `loglevel VERBOSE` or `loglevel INFO`:

```
# sshd -T | grep loglevel
loglevel VERBOSE
- OR -
loglevel INFO
```

- IF - Match set statements are used in your environment, specify the connection parameters to use for the `-T` extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user `sshuser`:*

```
# sshd -T -C user=sshuser | grep loglevel
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple `-C` options or as a comma-separated list. The keywords are `addr` (source address), `user` (user), `host` (resolved source host name), `laddr` (local address), `lport` (local port number), and `rdomain` (routing domain)

## **Remediation:**

Edit the `/etc/ssh/sshd_config` file to set the `LogLevel` parameter to `VERBOSE` or `INFO` above any `Include` and `Match` entries as follows:

```
LogLevel VERBOSE  
- OR -  
LogLevel INFO
```

**Note:** First occurrence of an option takes precedence, `Match` set statements notwithstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

## **Default Value:**

`LogLevel INFO`

## **References:**

1. [https://www.ssh.com/ssh/sshd\\_config/](https://www.ssh.com/ssh/sshd_config/)
2. NIST SP 800-53 Rev. 5: AU-3, AU-12, SI-5

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> 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	

### *5.1.15 Ensure sshd MACs are configured (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 approved are:
  - HMAC-SHA1
  - HMAC-SHA2-256
  - HMAC-SHA2-384
  - HMAC-SHA2-512

#### **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 to verify none of the "weak" MACs are being used:

```
# sshd -T | grep -Pi -- 'macs\h+([^\#\n\r]+,) ?(hmac-md5|hmac-md5-96|hmac-ripemd160|hmac-sha1-96|umac-64@openssh\.com|hmac-md5-etm@openssh\.com|hmac-md5-96-etm@openssh\.com|hmac-ripemd160-etm@openssh\.com|hmac-sha1-96-etm@openssh\.com|umac-64-etm@openssh\.com|umac-128-etm@openssh\.com)\b'
```

Nothing should be returned

**Note:** Review [CVE-2023-48795](#) and verify the system has been patched. If the system has not been patched, review the use of the Encrypt Then Mac (etm) MACs. The following are considered "weak" MACs, and should not be used:

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-sha1-96
umac-64@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
hmac-sha1-96-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 unapproved (weak) MACs preceded with a `-` above any

Include entries:

*Example:*

```
MACs -hmac-md5,hmac-md5-96,hmac-ripemd160,hmac-sha1-96,umac-64@openssh.com,hmac-md5-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com
```

- IF - [CVE-2023-48795](#) has not been reviewed and addressed, the following `etm` MACs should be added to the exclude list: `hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com`

**Note:** First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

## 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. <https://nvd.nist.gov/vuln/detail/CVE-2023-48795>
2. More information on SSH downgrade attacks can be found here:  
<http://www.mitls.org/pages/attacks/SLOTH>
3. SSHD\_CONFIG(5)
4. 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	<b>3.10 Encrypt Sensitive Data in Transit</b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 Encrypt All Sensitive Information in Transit</b> Encrypt all sensitive information in transit.		●	●
v7	<b>16.5 Encrypt Transmittal of Username and Authentication Credentials</b> 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

## 5.1.16 Ensure sshd MaxAuthTries is configured (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 `MaxAuthTries` is 4 or less:

```
# sshd -T | grep maxauthtries  
maxauthtries 4
```

- IF - `Match` set statements are used in your environment, specify the connection parameters to use for the `-T` extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user `sshuser`:*

```
# sshd -T -C user=sshuser | grep maxauthtries
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple `-C` options or as a comma-separated list. The keywords are `addr` (source address), `user` (user), `host` (resolved source host name), `laddr` (local address), `lport` (local port number), and `rdomain` (routing domain)

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `MaxAuthTries` parameter to 4 or less above any `Include` and `Match` entries as follows:

```
MaxAuthTries 4
```

**Note:** First occurrence of an option takes precedence, `Match` set statements notwithstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

**Default Value:**

MaxAuthTries 6

**References:**

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 Rev. 5: AU-3

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>16.13 Alert on Account Login Behavior Deviation</b> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

**MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.003	TA0006	M1036

## 5.1.17 Ensure sshd MaxSessions is configured (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 `MaxSessions` is 10 or less:

```
# sshd -T | grep -i maxsessions  
maxsessions 10
```

Run the following command and verify the output:

```
grep -Psi -- '^h*MaxSessions\h+\"?(1[1-9]|2-9)[0-9]|1-9)[0-9][0-9]+)\b'  
/etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf  
  
Nothing should be returned
```

- **IF** - `Match` set statements are used in your environment, specify the connection parameters to use for the `-T` extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user `sshuser`:*

```
# sshd -T -C user=sshuser | grep maxsessions
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple `-C` options or as a comma-separated list. The keywords are `addr` (source address), `user` (user), `host` (resolved source host name), `laddr` (local address), `lport` (local port number), and `rdomain` (routing domain)

## **Remediation:**

Edit the `/etc/ssh/sshd_config` file to set the `MaxSessions` parameter to 10 or less above any `Include` and `Match` entries as follows:

```
MaxSessions 10
```

**Note:** First occurrence of an option takes precedence, `Match` set statements notwithstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

## **Default Value:**

MaxSessions 10

## **References:**

1. SSSH\_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## **MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.002	TA0040	

## 5.1.18 Ensure sshd 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 to verify `MaxStartups` is `10:30:60` or more restrictive:

```
# sshd -T | awk '$1 ~ /^maxstartups/{split($2, a, ":");{if(a[1] > 10 || a[2] > 30 || a[3] > 60) print $0}}'
```

Nothing should be returned

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `MaxStartups` parameter to `10:30:60` or more restrictive above any `Include` entries as follows:

```
MaxStartups 10:30:60
```

**Note:** First occurrence of a option takes precedence. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

### Default Value:

`MaxStartups 10:30:100`

### References:

1. `SSHD_CONFIG(5)`
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**MITRE ATT&CK Mappings:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1499, T1499.002	TA0040	

## 5.1.19 Ensure sshd 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 to verify `PermitEmptyPasswords` is set to no:

```
# sshd -T | grep permitemptypasswords
permitemptypasswords no
```

- IF - `Match` set statements are used in your environment, specify the connection parameters to use for the `-T` extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user `sshuser`:*

```
# sshd -T -C user=sshuser | grep permitemptypasswords
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple `-C` options or as a comma-separated list. The keywords are `addr` (source address), `user` (user), `host` (resolved source host name), `laddr` (local address), `lport` (local port number), and `rdomain` (routing domain)

### Remediation:

Edit `/etc/ssh/sshd_config` and set the `PermitEmptyPasswords` parameter to no above any `Include` and `Match` entries as follows:

```
PermitEmptyPasswords no
```

**Note:** First occurrence of an option takes precedence, `Match` set statements notwithstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

**Default Value:**

PermitEmptyPasswords no

**References:**

1. SSHD\_CONFIG(5)
2. 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	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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
T1021	TA0008	M1042

## 5.1.20 Ensure sshd PermitRootLogin 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 to verify `PermitRootLogin` is set to `no`:

```
# sshd -T | grep permitrootlogin  
permitrootlogin no
```

- IF - Match set statements are used in your environment, specify the connection parameters to use for the `-T` extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user `sshuser`:*

```
# sshd -T -C user=sshuser | grep permitrootlogin
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple `-C` options or as a comma-separated list. The keywords are `addr` (source address), `user` (user), `host` (resolved source host name), `laddr` (local address), `lport` (local port number), and `rdomain` (routing domain)

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `PermitRootLogin` parameter to `no` above any `Include` and `Match` entries as follows:

```
PermitRootLogin no
```

**Note:** First occurrence of an option takes precedence, `Match` set statements notwithstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

**Default Value:**

PermitRootLogin without-password

**References:**

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 Rev. 5:AC-6

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</b></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><b>4.3 Ensure the Use of Dedicated Administrative Accounts</b></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

## *5.1.21 Ensure sshd 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 to verify `PermitUserEnvironment` is set to no:

```
# sshd -T | grep permituserenvironment
permituserenvironment no
```

### **Remediation:**

Edit the `/etc/ssh/sshd_config` file to set the `PermitUserEnvironment` parameter to no above any `Include` entries as follows:

```
PermitUserEnvironment no
```

**Note:** First occurrence of an option takes precedence. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

### **Default Value:**

`PermitUserEnvironment no`

### **References:**

1. `SSHD_CONFIG(5)`
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5
3. `SSHD(8)`

**MITRE ATT&CK Mappings:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1021	TA0008	M1042

## 5.1.22 Ensure sshd UsePAM 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 to verify `UsePAM` is set to `yes`:

```
# sshd -T | grep -i usepam  
usepam yes
```

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `UsePAM` parameter to `yes` above any `Include` entries as follows:

```
UsePAM yes
```

**Note:** First occurrence of an option takes precedence. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

### Default Value:

`UsePAM yes`

### References:

1. `SSHD_CONFIG(5)`
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5
3. `SSHD(8)`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.2 Use Unique Passwords</b>            Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.</p>	●	●	●
v7	<p><b>4.4 Use Unique Passwords</b>            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>		●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021, T1021.004	TA0001	M1035

## 5.2 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`.

### *5.2.1 Ensure sudo is installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **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:**

Run the following command to verify that either `sudo` is installed:

```
# dpkg-query -s sudo &>/dev/null && echo "sudo is installed"  
sudo is installed
```

**- OR -**

Run the following command to verify that either `sudo-ldap` is installed:

```
# dpkg-query -s sudo-ldap &>/dev/null && echo "sudo-ldap is installed"  
sudo-ldap is 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)
2. NIST SP 800-53 Rev. 5: AC-6

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b> 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	<b>4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u></b> 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.	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548	TA0004	M1026

## 5.2.2 Ensure sudo commands use pty (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

`sudo` can be configured to run only from a pseudo 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 to verify `Defaults use_pty` is set:

```
# grep -rPi -- '^h*Defaults\h+([^\#\n\r]+,)?use_pty(,\h*\h+\h*)*\h*(#.*)?$$' /etc/sudoers*
```

Verify the output matches:

```
/etc/sudoers:Defaults use_pty
```

Run the follow command to to verify `Defaults !use_pty` is not set:

```
# grep -rPi -- '^h*Defaults\h+([^\#\n\r]+,)?!use_pty(,\h*\h+\h*)*\h*(#.*)?$$' /etc/sudoers*
```

Nothing should be returned

## **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
```

Edit the file /etc/sudoers with visudo and any files in /etc/sudoers.d/ with visudo -f <PATH TO FILE> and remove any occurrence of !use\_pty

### **Note:**

- sudo will read each file in /etc/sudoers.d, skipping file names that end in ~ or contain a . character to avoid causing problems with package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, /etc/sudoers.d/01\_first will be parsed before /etc/sudoers.d/10\_second.
- Be aware that because the sorting is lexical, not numeric, /etc/sudoers.d/1\_whoops would be loaded after /etc/sudoers.d/10\_second.
- Using a consistent number of leading zeroes in the file names can be used to avoid such problems.

## **References:**

1. SUDO(8)
2. VISUDO(8)
3. sudoers(5)
4. NIST SP 800-53 Rev. 5: AC-6

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</b> 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	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

**MITRE ATT&CK Mappings:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1078, T1078.003, T1548, T1548.003	TA0001, TA0003	M1026, M1028

### 5.2.3 Ensure sudo log file exists (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

sudo can use a custom log file

#### 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"
```

#### Note:

- sudo will read each file in `/etc/sudoers.d`, skipping file names that end in ~ or contain a . character to avoid causing problems with package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, `/etc/sudoers.d/01_first` will be parsed before `/etc/sudoers.d/10_second`.
- Be aware that because the sorting is lexical, not numeric, `/etc/sudoers.d/1_whoops` would be loaded after `/etc/sudoers.d/10_second`.
- Using a consistent number of leading zeroes in the file names can be used to avoid such problems.

## References:

1. SUDO(8)
2. VISUDO(8)
3. sudoers(5)
4. NIST SP 800-53 Rev. 5: AU-3, AU-12

## 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	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>6.3 Enable Detailed Logging</b> 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	TA0004	M1026

## *5.2.4 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.

### **References:**

1. NIST SP 800-53 Rev. 5: AC-6

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</b></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><b>4.3 Ensure the Use of Dedicated Administrative Accounts</b></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
T1548	TA0004	M1026

## *5.2.5 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).

### **References:**

1. NIST SP 800-53 Rev. 5: AC-6

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b></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><b>4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u></b></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
T1548	TA0004	M1026

## *5.2.6 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 its 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>
2. NIST SP 800-53 Rev. 5: AC-6

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</b> 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	<b>4.3 Ensure the Use of Dedicated Administrative Accounts</b> 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.	●	●	●

## **MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1548	TA0004	M1026

## 5.2.7 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[ ]+use_uid[ ]+group=[^#\'\n\r]+[ ]+group_name' /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
```

## **References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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	TA0005	M1026

### **5.3 Pluggable Authentication Modules**

### **5.3.1 Configure PAM software packages**

Updated versions of PAM include additional functionality

### *5.3.1.1 Ensure latest version of pam is installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Updated versions of PAM include additional functionality

#### **Rationale:**

To ensure the system has full functionality and access to the options covered by this Benchmark the latest version of `libpam-runtime` should be installed on the system

#### **Audit:**

Run the following command to verify the version of `libpam-runtime` on the system:

```
# dpkg-query -s libpam-runtime | grep -P -- '^^(Status|Version)\b'
```

The output should be similar to:

```
Status: install ok installed
Version: 1.4.0-9
```

#### **Remediation:**

- IF - the version of `libpam-runtime` on the system is less than version 1.5.2-6:  
Run the following command to update to the latest version of PAM:

```
# apt upgrade libpam-runtime
```

### *5.3.1.2 Ensure libpam-modules is installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Pluggable Authentication Modules for PAM

#### **Rationale:**

To ensure the system has full functionality and access to the PAM options covered by this Benchmark

#### **Audit:**

Run the following command to verify `libpam-modules` is installed and version 1.5.2-6 or later:

```
# dpkg-query -s libpam-modules | grep -P -- '^^(Status|Version)\b'
```

The output should be similar to:

```
Status: install ok installed
Version: 1.4.0-9
```

#### **Remediation:**

- IF - the version of `libpam-modules` on the system is less than version 1.5.2-6:  
Run the following command to update to the latest version of PAM:

```
# apt upgrade libpam-modules
```

### *5.3.1.3 Ensure libpam-pwquality is installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

`libpwquality` provides common functions for password quality checking and scoring them based on their apparent randomness. The library also provides a function for generating random passwords with good pronounceability.

This module can be plugged into the password stack of a given service to provide some plug-in strength-checking for passwords. The code was originally based on `pam_cracklib` module and the module is backwards compatible with its options.

#### **Rationale:**

Strong passwords reduce the risk of systems being hacked through brute force methods.

#### **Audit:**

Run the following command to verify `libpam-pwquality` is installed:

```
# dpkg-query -s libpam-pwquality | grep -P -- '^_Status|Version)\b'
```

The output should be similar to:

```
Status: install ok installed
Version: 1.4.4-1
```

#### **Remediation:**

Run the following command to install `libpam-pwquality`:

```
# apt install libpam-pwquality
```

#### **References:**

1. <https://packages.debian.org/buster/libpam-pwquality>

### 5.3.2 Configure pam-auth-update profiles

`pam-auth-update` is a utility that permits configuring the central authentication policy for the system using pre-defined profiles as supplied by PAM module packages.

Profiles - Shipped in the `/usr/share/pam-configs/` directory specify the modules, with options, to enable; the preferred ordering with respect to other profiles; and whether a profile should be enabled by default. Packages providing PAM modules register their profiles at install time by calling `pam-auth-update --package`.

Selection of profiles is done using the standard `debconf` interface. The profile selection question will be asked at `medium` priority when packages are added or removed, so no user interaction is required by default. Users may invoke `pam-auth-update` directly to change their authentication configuration.

The `pam-auth-update` script makes every effort to respect local changes to `/etc/pam.d/common-*`. Local modifications to the list of module options will be preserved, and additions of modules within the managed portion of the stack will cause `pam-auth-update` to treat the config files as locally modified and not make further changes to the config files unless given the `--force` option.

If the user specifies that `pam-auth-update` should override local configuration changes, the locally-modified files will be saved in `/etc/pam.d/` with a suffix of `.pam-old`.

### *5.3.2.1 Ensure pam\_unix module is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

pam\_unix is the standard Unix authentication module. It uses standard calls from the system's libraries to retrieve and set account information as well as authentication. Usually this is obtained from the /etc/passwd and if shadow is enabled, the /etc/shadow file as well.

The account component performs the task of establishing the status of the user's account and password based on the following shadow elements: expire, last\_change, max\_change, min\_change, warn\_change. In the case of the latter, it may offer advice to the user on changing their password or, through the PAM\_AUTHTOKEN\_REQD return, delay giving service to the user until they have established a new password. The entries listed above are documented in the shadow(5) manual page. Should the user's record not contain one or more of these entries, the corresponding shadow check is not performed.

The authentication component performs the task of checking the users credentials (password). The default action of this module is to not permit the user access to a service if their official password is blank.

#### **Rationale:**

The system should only provide access after performing authentication of a user.

#### **Audit:**

Run the following command to verify that pam\_unix is enabled:

```
# grep -P -- '\bpam_unix\.so\b' /etc/pam.d/common-  
{account,session,auth,password}
```

Output should be simular to:

```
/etc/pam.d/common-account:account      [success=1 new_authtok_reqd=done  
default=ignore]      pam_unix.so  
/etc/pam.d/common-session:session      required      pam_unix.so  
/etc/pam.d/common-auth:auth      [success=2 default=ignore]      pam_unix.so  
try_first_pass  
/etc/pam.d/common-password:password      [success=1 default=ignore]  
pam_unix.so obscure use_authtok try_first_pass yescrypt
```

## Remediation:

Run the following command to enable the `pam_unix` module:

```
# pam-auth-update --enable unix
```

**Note:** If a site specific custom profile is being used in your environment to configure PAM that includes the configuration for the `pam_faillock` module, enable that module instead

## References:

1. NIST SP 800-53 Rev. 5: IA-5(1)

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

### *5.3.2.2 Ensure pam\_faillock module is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `pam_faillock.so` module maintains a list of failed authentication attempts per user during a specified interval and locks the account in case there were more than the configured number of consecutive failed authentications (this is defined by the `deny` parameter in the faillock configuration). It stores the failure records into per-user files in the `tally` directory.

#### **Rationale:**

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

#### **Audit:**

Run the following commands to verify that `pam_faillock` is enabled:

```
# grep -P -- '\bpam_faillock\.so\b' /etc/pam.d/common-{auth,account}
```

Output should be similar to:

```
/etc/pam.d/common-auth:auth      requisite
pam_faillock.so preauth
/etc/pam.d/common-auth:auth      [default=die]
pam_faillock.so authfail
/etc/pam.d/common-account:account      required
pam_faillock.so
```

## Remediation:

Create two pam-auth-update profiles in /usr/share/pam-configs/:  
Create the first profile with the following lines:

```
Name: Enable pam_faillock to deny access
Default: yes
Priority: 0
Auth-Type: Primary
Auth:
    [default=die]                               pam_faillock.so authfail
```

*Example:*

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

{
    arr=('Name: Enable pam_faillock to deny access' 'Default: yes' 'Priority:
0' 'Auth-Type: Primary' 'Auth:' '        [default=die]
pam_faillock.so authfail')
    printf '%s\n' "${arr[@]}" > /usr/share/pam-configs/faillock
}
```

Create the second profile with the following lines:

```
Name: Notify of failed login attempts and reset count upon success
Default: yes
Priority: 1024
Auth-Type: Primary
Auth:
    requisite                           pam_faillock.so preauth
Account-Type: Primary
Account:
    required                            pam_faillock.so
```

*Example:*

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

{
    arr=('Name: Notify of failed login attempts and reset count upon success'
'Default: yes' 'Priority: 1024' 'Auth-Type: Primary' 'Auth:' 'requisite
pam_faillock.so preauth' 'Account-Type:
Primary' 'Account:' '        required
pam_faillock.so')
    printf '%s\n' "${arr[@]}" > /usr/share/pam-configs/faillock_notify
}
```

Run the following command to update the common-auth and common-account PAM files with the new profiles:

```
# pam-auth-update --enable <profile_filename>
```

*Example:*

```
# pam-auth-update --enable faillock
# pam-auth-update --enable faillock_notify
```

**Note:**

- The name used for the file must be used in the `pam-auth-update --enable` command
- The `Name:` line should be easily recognizable and understood
- The `Priority:` Line is important as it effects the order of the lines in the `/etc/pam.d/` files
- If a site specific custom profile is being used in your environment to configure PAM that includes the configuration for the `pam_faillock` module, enable that module instead

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.2 Establish an Access Revoking Process</b> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	<b>16.7 Establish Process for Revoking Access</b> 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

### *5.3.2.3 Ensure pam\_pwquality module is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `pam_pwquality.so` module performs password quality checking. This module can be plugged into the password stack of a given service to provide strength-checking for passwords. The code was originally based on `pam_cracklib` module and the module is backwards compatible with its options.

The action of this module is to prompt the user for a password and check its strength against a system dictionary and a set of rules for identifying poor choices.

The first action is to prompt for a single password, check its strength and then, if it is considered strong, prompt for the password a second time (to verify that it was typed correctly on the first occasion). All being well, the password is passed on to subsequent modules to be installed as the new authentication token.

#### **Rationale:**

Use of a unique, complex passwords helps to increase the time and resources required to compromise the password.

#### **Audit:**

Run the following command to verify that `pam_pwhistory` is enabled:

```
# grep -P -- '\bpam_pwquality\.so\b' /etc/pam.d/common-password
```

Output should be similar to:

```
password    requisite    pam_pwquality.so  retry=3
```

## **Remediation:**

Run the following script to verify the `pam_pwquality.so` line exists in a `pam-auth-update` profile:

```
# grep -P -- '\bpam_pwquality\.so\b' /usr/share/pam-configs/*
```

Output should be similar to:

```
/usr/share/pam-configs/pwquality:      requisite  
pam_pwquality.so retry=3  
/usr/share/pam-configs/pwquality:      requisite  
pam_pwquality.so retry=3
```

- IF - similar output is returned:

Run the following command to update `/etc/pam.d/common-password` with the returned profile:

```
# pam-auth-update --enable {PROFILE_NAME}
```

*Example:*

```
# pam-auth-update pwquality
```

- IF - similar output is NOT returned:

Run the following script to create a `pam-auth-update` profile for `pwquality`:

```
#!/usr/bin/env bash  
  
{  
    arr=('Name: Pwquality password strength checking' 'Default: yes'  
'Priority: 1024' 'Conflicts: cracklib' 'Password-Type: Primary' 'Password:' ''  
requisite  
        pam_pwquality.so retry=3' 'Password-Initial:'  
'requisite')  
    printf '%s\n' "${arr[@]}" > /usr/share/pam-configs/pwquality  
}
```

Run the following command to update `/etc/pam.d/common-password` with the `pwquality` profile:

```
# pam-auth-update --enable pwquality
```

**Note:**

- The name used for the file must be used in the `pam-auth-update --enable` command
- The `Name:` line should be easily recognizable and understood
- The `Priority:` Line is important as it effects the order of the lines in the `/etc/pam.d/` files
- If a site specific custom profile is being used in your environment to configure PAM that includes the configuration for the `pam_pwquality` module, enable that module instead

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.2 Use Unique Passwords</b>            Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.</p>	●	●	●
v7	<p><b>4.4 Use Unique Passwords</b>            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>		●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

### *5.3.2.4 Ensure pam\_pwhistory module is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `pam_pwhistory.so` module saves the last passwords for each user in order to force password change history and keep the user from alternating between the same password too frequently.

This module does not work together with kerberos. In general, it does not make much sense to use this module in conjunction with `NIS` or `LDAP`, since the old passwords are stored on the local machine and are not available on another machine for password history checking.

#### **Rationale:**

Use of a unique, complex passwords helps to increase the time and resources required to compromise the password.

#### **Audit:**

Run the following command to verify that `pam_pwhistory` is enabled:

```
# grep -P -- '\bpam_pwhistory\.so\b' /etc/pam.d/common-password
```

Output should be similar to:

```
password    requisite    pam_pwhistory.so remember=24 enforce_for_root
try_first_pass use_authok
```

## **Remediation:**

Run the following script to verify the `pam_pwquality.so` line exists in a `pam-auth-update` profile:

```
# grep -P -- '\bpam_pwhistory\.so\b' /usr/share/pam-configs/*
```

Output should be similar to:

```
/usr/share/pam-configs/pwhistory:    requisite    pam_pwhistory.so remember=24
enforce_for_root try_first_pass use_authtok
```

- IF - similar output is returned:

Run the following command to update `/etc/pam.d/common-password` with the returned profile:

```
# pam-auth-update --enable {PROFILE_NAME}
```

*Example:*

```
# pam-auth-update pwhistory
```

- IF - similar output is NOT returned:

Run the following script to create a `pam-auth-update` profile for `pwhistory`:

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

{
    arr=('Name: pwhistory password history checking' 'Default: yes' 'Priority:
1024' 'Password-Type: Primary' 'Password:' '        requisite
pam_pwhistory.so remember=24 enforce_for_root try_first_pass use_authtok')
    printf '%s\n' "${arr[@]}" > /usr/share/pam-configs/pwhistory
}
```

Run the following command to update `/etc/pam.d/common-password` with the `pwhistory` profile:

```
# pam-auth-update --enable pwhistory
```

**Note:**

- The name used for the file must be used in the `pam-auth-update --enable` command
- The `Name:` line should be easily recognizable and understood
- The `Priority:` Line is important as it effects the order of the lines in the `/etc/pam.d/` files
- If a site specific custom profile is being used in your environment to configure PAM that includes the configuration for the `pam_pwhistory` module, enable that module instead

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.</p>	●	●	●
v7	<p><b>4.4 Use Unique Passwords</b> 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>		●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

### 5.3.3 Configure PAM Arguments

Pluggable Authentication Modules (PAM) uses arguments to pass information to a pluggable module during authentication for a particular module type. These arguments allow the PAM configuration files for particular programs to use a common PAM module but in different ways.

Invalid arguments are ignored and do not otherwise affect the success or failure of the PAM module. When an invalid argument is passed, an error is usually written to `/var/log/messages` file. However, since the reporting method is controlled by the PAM module, the module must be written correctly to log the error to this file.

**Note:** If custom PAM files are being used, for this section's remediation, the corresponding files in `/etc/pam.d/` would need to be edited directly, and the `pam-auth-update --enable <EDITED_PROFILE_NAME>` command skipped

### 5.3.3.1 Configure pam\_faillock module

`pam_faillock.so` provides a way to configure the default settings for locking the user after multiple failed authentication attempts.

Options:

- `<dir=/path/to/tally-directory>` - The directory where the user files with the failure records are kept. The default is `/var/run/faillock`. Note: These files will disappear after reboot on systems configured with directory `/var/run/faillock` mounted on virtual memory.
- `audit` - Will log the user name into the system log if the user is not found.
- `silent` - Don't print informative messages to the user. Please note that when this option is not used there will be difference in the authentication behavior for users which exist on the system and non-existing users.
- `no_log_info` - Don't log informative messages via `syslog(3)`.
- `local_users_only` - Only track failed user authentications attempts for local users in `/etc/passwd` and ignore centralized (AD, IdM, LDAP, etc.) users. The `faillock(8)` command will also no longer track user failed authentication attempts. Enabling this option will prevent a double-lockout scenario where a user is locked out locally and in the centralized mechanism.
- `nodelay` - Don't enforce a delay after authentication failures.
- `deny=<n>` - Deny access if the number of consecutive authentication failures for this user during the recent interval exceeds . The default is 3.
- `fail_interval=n` - The length of the interval during which the consecutive authentication failures must happen for the user account lock out is n seconds. The default is 900 (15 minutes).
- `unlock_time=n` - The access will be re-enabled after n seconds after the lock out. The value 0 has the same meaning as value never - the access will not be re-enabled without resetting the faillock entries by the `faillock(8)` command. The default is 600 (10 minutes). Note that the default directory that `pam_faillock` uses is usually cleared on system boot so the access will be also re-enabled after system reboot. If that is undesirable a different tally directory must be set with the `dir` option. Also note that it is usually undesirable to permanently lock out users as they can become easily a target of denial of service attack unless the usernames are random and kept secret to potential attackers.
- `even_deny_root` - Root account can become locked as well as regular accounts.
- `root_unlock_time=n` - This option implies `even_deny_root` option. Allow access after n seconds to root account after the account is locked. In case the option is not specified the value is the same as of the `unlock_time` option.
- `admin_group=name` - If a group name is specified with this option, members of the group will be handled by this module the same as the root account (the options `even_deny_root` and `root_unlock_time` will apply to them. By default the option is not set.

### *5.3.3.1.1 Ensure password failed attempts lockout is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `deny=<n>` option will deny access if the number of consecutive authentication failures for this user during the recent interval exceeds .

#### **Rationale:**

Locking out user IDs after *n* unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

#### **Audit:**

Run the following command to verify that Number of failed logon attempts before the account is locked is no greater than 5 and meets local site policy:

```
# grep -Pi -- '^h*deny\h*=\h*[1-5]\b' /etc/security/faillock.conf  
deny = 5
```

Run the following command to verify that the `deny` argument has not been set, or 5 or less and meets local site policy:

```
# grep -Pi -- '^h*auth\h+(requisite|required|sufficient)\h+pam_faillock\.so\h+([^\#\n\r]+)\h+\)?deny\h*=\h*(0|[6-9]|1-9)[0-9]+\b' /etc/pam.d/common-auth  
Nothing should be returned
```

#### **Remediation:**

Create or edit the following line in `/etc/security/faillock.conf` setting the `deny` option to 5 or less:

```
deny = 5
```

Run the following command:

```
# grep -Pl -- '\bpam_faillock\.so\h+([^\#\n\r]+)\h+\)?deny\b' /usr/share/pam-configs/*
```

Edit any returned files and remove the `deny=<N>` arguments from the `pam_faillock.so` line(s):

**Default Value:**

deny = 3

**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 `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
v8	<b>6.2 Establish an Access Revoking Process</b> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	<b>16.7 Establish Process for Revoking Access</b> 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

### *5.3.3.1.2 Ensure password unlock time is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

`unlock_time=<n>` - The access will be re-enabled after seconds after the lock out. The value 0 has the same meaning as value never - the access will not be re-enabled without resetting the faillock entries by the faillock(8) command.

#### **Note:**

- The default directory that pam\_faillock uses is usually cleared on system boot so the access will be also re-enabled after system reboot. If that is undesirable a different tally directory must be set with the dir option.
- It is usually undesirable to permanently lock out users as they can become easily a target of denial of service attack unless the usernames are random and kept secret to potential attackers.
- The maximum configurable value for `unlock_time` is 604800

#### **Rationale:**

Locking out user IDs after  $n$  unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

#### **Impact:**

Use of `unlock_time=0` may allow an attacker to cause denial of service to legitimate users. This will also require a systems administrator with elevated privileges to unlock the account.

## Audit:

Run the following command to verify that the time in seconds before the account is unlocked is either 0 (never) or 900 (15 minutes) or more and meets local site policy:

```
# grep -Pi -- '^h*unlock_time\h*=\h*(0|9[0-9][0-9]|1-9[0-9]{3,})\b' /etc/security/faillock.conf  
unlock_time = 900
```

Run the following command to verify that the `unlock_time` argument has not been set, or is either 0 (never) or 900 (15 minutes) or more and meets local site policy:

```
# grep -Pi -- '^h*auth\h+(requisite|required|sufficient)\h+pam_faillock\.so\h+([^\#\n\r]+\h+)\?unlock_time\h*=\h*([1-9]|1-9[0-9]|1-8[0-9][0-9])\b' /etc/pam.d/common-auth  
  
Nothing should be returned
```

## Remediation:

Set password unlock time to conform to site policy. `unlock_time` should be 0 (never), or 900 seconds or greater.

Edit `/etc/security/faillock.conf` and update or add the following line:

```
unlock_time = 900
```

Run the following command: remove the `unlock_time` argument from the `pam_faillock.so` module in the PAM files:

```
# grep -Pl -- '\bpam_faillock\.so\h+([^\#\n\r]+\h+)\?unlock_time\b' /usr/share/pam-configs/*
```

Edit any returned files and remove the `unlock_time=<N>` argument from the `pam_faillock.so` line(s):

## Default Value:

`unlock_time = 600`

## 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 `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
v8	<p><b>6.2 Establish an Access Revoking Process</b>  Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.</p>	●	●	●
v7	<p><b>16.7 Establish Process for Revoking Access</b>  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>		●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.003	TA0006	M1027

### *5.3.3.1.3 Ensure password failed attempts lockout includes root account (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

`even_deny_root` - Root account can become locked as well as regular accounts

`root_unlock_time=n` - This option implies `even_deny_root` option. Allow access after n seconds to root account after the account is locked. In case the option is not specified the value is the same as of the `unlock_time` option.

#### **Rationale:**

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

#### **Impact:**

Use of `unlock_time=0` or `root_unlock_time=0` may allow an attacker to cause denial of service to legitimate users.

## Audit:

Run the following command to verify that `even_deny_root` and/or `root_unlock_time` is enabled:

```
# grep -Pi -- '^\\h*(even_deny_root|root_unlock_time)\\h*=\\h*\\d+\\b' /etc/security/faillock.conf
```

*Example output:*

```
even_deny_root  
--AND/OR--  
root_unlock_time = 60
```

Run the following command to verify that - **IF** - `root_unlock_time` is set, it is set to 60 (One minute) or more:

```
# grep -Pi -- '^\\h*root_unlock_time\\h*=\\h*([1-9] | [1-5][0-9])\\b' /etc/security/faillock.conf
```

```
Nothing should be returned
```

Run the following command to check the `pam_faillock.so` module for the `root_unlock_time` argument. Verify - **IF**- `root_unlock_time` is set, it is set to 60 (One minute) or more:

```
# grep -Pi -- '^\\h*auth\\h+([\\^#\\n\\r]+\\h+)pam_faillock\\.so\\h+([\\^#\\n\\r]+\\h+)?root_unlock_time\\h*=\\h*([1-9] | [1-5][0-9])\\b' /etc/pam.d/common-auth
```

```
Nothing should be returned
```

## Remediation:

Edit `/etc/security/faillock.conf`:

- Remove or update any line containing `root_unlock_time`, - **OR** - set it to a value of 60 or more
- Update or add the following line:

```
even_deny_root
```

Run the following command:

```
# grep -Pl -- '\\bpam_faillock\\.so\\h+([\\^#\\n\\r]+\\h+)?(even_deny_root|root_unlock_time)' /usr/share/pam-configs/*
```

Edit any returned files and remove the `even_deny_root` and `root_unlock_time` arguments from the `pam_faillock.so` line(s):

**Default Value:**

disabled

**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 `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
v8	<b>6.2 Establish an Access Revoking Process</b> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	<b>16.7 Establish Process for Revoking Access</b> 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

### 5.3.3.2 Configure pam\_pwquality module

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.

These checks are configurable by either:

- use of the module arguments
- modifying the `/etc/security/pwquality.conf` configuration file
- creating a `.conf` file in the `/etc/security/pwquality.conf.d/` directory.

**Note:** The module arguments override the settings in the `/etc/security/pwquality.conf` configuration file. Settings in the `/etc/security/pwquality.conf` configuration file override settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory.

The possible options in the file are:

- `difok` - Number of characters in the new password that must not be present in the old password. (default 1). The special value of 0 disables all checks of similarity of the new password with the old password except the new password being exactly the same as the old one.
- `minlen` - Minimum acceptable size for the new password (plus one if credits are not disabled which is the default). (See `pam_pwquality(8)`.) Cannot be set to lower value than 6. (default 8)
- `dcredit` - The maximum credit for having digits in the new password. If less than 0 it is the minimum number of digits in the new password. (default 0)
- `ucredit` - The maximum credit for having uppercase characters in the new password. If less than 0 it is the minimum number of uppercase characters in the new password. (default 0)
- `lcredit` - The maximum credit for having lowercase characters in the new password. If less than 0 it is the minimum number of lowercase characters in the new password. (default 0)
- `ocredit` - The maximum credit for having other characters in the new password. If less than 0 it is the minimum number of other characters in the new password. (default 0)
- `minclass` - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others). (default 0)
- `maxrepeat` - The maximum number of allowed same consecutive characters in the new password. The check is disabled if the value is 0. (default 0)
- `maxsequence` - The maximum length of monotonic character sequences in the new password. Examples of such sequence are '12345' or 'fedcb'. Note that most such passwords will not pass the simplicity check unless the sequence is only a minor part of the password. The check is disabled if the value is 0. (default 0)

- `maxclassrepeat` - The maximum number of allowed consecutive characters of the same class in the new password. The check is disabled if the value is 0. (default 0)
- `gecoscheck` - If nonzero, check whether the words longer than 3 characters from the GECOS field of the user's passwd(5) entry are contained in the new password. The check is disabled if the value is 0. (default 0)
- `dictcheck` - If nonzero, check whether the password (with possible modifications) matches a word in a dictionary. Currently the dictionary check is performed using the cracklib library. (default 1)
- `usercheck=<N>` - If nonzero, check whether the password (with possible modifications) contains the user name in some form. It is not performed for user names shorter than 3 characters. (default 1)
- `usersubstr=<N>` - If greater than 3 (due to the minimum length in usercheck), check whether the password contains a substring of at least N length in some form. (default 0)
- `enforcing=<N>` - If nonzero, reject the password if it fails the checks, otherwise only print the warning. This setting applies only to the pam\_pwquality module and possibly other applications that explicitly change their behavior based on it. It does not affect pwmake(1) and pwscore(1). (default 1)
- `badwords` - Space separated list of words that must not be contained in the password. These are additional words to the cracklib dictionary check. This setting can be also used by applications to emulate the gecos check for user accounts that are not created yet.
- `dictpath` - Path to the cracklib dictionaries. Default is to use the cracklib default.
- `retry=<N>` - Prompt user at most N times before returning with error. The default is 1.
- `enforce_for_root` - The module will return error on failed check even if the user changing the password is root. This option is off by default which means that just the message about the failed check is printed but root can change the password anyway. Note that root is not asked for an old password so the checks that compare the old and new password are not performed.
- `local_users_only` - The module will not test the password quality for users that are not present in the /etc/passwd file. The module still asks for the password so the following modules in the stack can use the use\_authok option. This option is off by default.

### *5.3.3.2.1 Ensure password number of changed characters is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `pwquality difok` option sets the number of characters in a password that must not be present in the old password.

#### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

## Audit:

Run the following command to verify that the `difok` option is set to 2 or more and follows local site policy:

```
# grep -Psi -- '^h*difok\h*=\h*([2-9]|1-9[0-9]+)\b'  
/etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

*Example output:*

```
/etc/security/pwquality.conf.d/50-pwdifok.conf:difok = 2
```

Verify returned value(s) are 2 or more and meet local site policy

Run the following command to verify that `difok` is not set, is 2 or more, and conforms to local site policy:

```
grep -Psi -- '^h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([^\#\n\r]+\h+)\?difok\h*=\h*([0-1])\b' /etc/pam.d/common-password
```

```
Nothing should be returned
```

## Note:

- settings should be configured in only **one** location for clarity
- Settings observe an order of precedence:
  - module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
  - settings in the `/etc/security/pwquality.conf` configuration file override settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory
  - settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory for clarity, convenience, and durability.

## **Remediation:**

Create or modify a file ending in .conf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line to set difok to 2 or more. Ensure setting conforms to local site policy:

**Example:**

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

{
    sed -ri 's/^s*difok\s*/# &/' /etc/security/pwquality.conf
    [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir
/etc/security/pwquality.conf.d/
    printf '\n%s' "difok = 2" > /etc/security/pwquality.conf.d/50-pwdifok.conf
}
```

Run the following command:

```
# grep -Pl -- '\bpam_pwquality\.so\h+([^\#\n\r]+\h+)\?difok\b' /usr/share/pam-configs/*
```

Edit any returned files and remove the difok argument from the pam\_pwquality.so line(s):

## **Default Value:**

difok = 1

## **References:**

1. NIST SP 800-53 Rev. 5: IA-5

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

### *5.3.3.2.2 Ensure minimum password length is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The minimum password length setting determines the lowest number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "passphrase" is a better term than "password".

The `minlen` option sets the minimum acceptable size for the new password (plus one if credits are not disabled which is the default). Cannot be set to lower value than 6.

#### **Rationale:**

Strong passwords help protect systems from password attacks. Types of password attacks include dictionary attacks, which attempt to use common words and phrases, and brute force attacks, which try every possible combination of characters. Also attackers may try to obtain the account database so they can use tools to discover the accounts and passwords.

#### **Impact:**

In general, it is true that longer passwords are better (harder to crack), but it is also true that forced password length requirements can cause user behavior that is predictable and undesirable. For example, requiring users to have a minimum 16-character password may cause them to choose repeating patterns like fourfourfourfour or passwordpassword that meet the requirement but aren't hard to guess. Additionally, length requirements increase the chances that users will adopt other insecure practices, like writing them down, re-using them or storing them unencrypted in their documents.

Having a reasonable minimum length with no maximum character limit increases the resulting average password length used (and therefore the strength).<sup>6</sup>

## Audit:

Run the following command to verify that password length is 14 or more characters, and conforms to local site policy:

```
# grep -Psi -- '^h*minlen\h*=\h*(1[4-9]|2-9][0-9]|1-9][0-9]{2,})\b' /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

*Example output:*

```
/etc/security/pwquality.conf.d/50-pwlenth.conf:minlen = 14
```

Verify returned value(s) are no less than 14 characters and meet local site policy

Run the following command to verify that minlen is not set, or is 14 or more characters, and conforms to local site policy:

```
grep -Psi -- '^h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([^\#\n\r]+\h+)\?minlen\h*=\h*([0-9]|1[0-3])\b' /etc/pam.d/system-auth /etc/pam.d/common-password
```

Nothing should be returned

## Note:

- settings should be configured in only **one** location for clarity
- Settings observe an order of precedence:
  - module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
  - settings in the `/etc/security/pwquality.conf` configuration file override settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory
  - settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory for clarity, convenience, and durability.

## **Remediation:**

Create or modify a file ending in `.conf` in the `/etc/security/pwquality.conf.d/` directory or the file `/etc/security/pwquality.conf` and add or modify the following line to set password length of 14 or more characters. Ensure that password length conforms to local site policy:

*Example:*

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

{
    sed -ri 's/^s*minlen\s*/# &/' /etc/security/pwquality.conf
    [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir
/etc/security/pwquality.conf.d/
    printf '\n%s' "minlen = 14" > /etc/security/pwquality.conf.d/50-
pwlength.conf
}
```

Run the following command:

```
# grep -Pl -- '\bpam_pwquality\.so\h+([^\#\n\r]+\h+)\?minlen\b' /usr/share/pam-
configs/*
```

Edit any returned files and remove the `minlen` argument from the `pam_pwquality.so` line(s):

## **Default Value:**

`minlen = 8`

## **References:**

1. [pam\\_pwquality\(8\)](#)
2. [CIS Password Policy Guide](#)
3. [NIST SP 800-53 Rev. 5: IA-5\(1\)](#)

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

### *5.3.3.2.3 Ensure password complexity is configured (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Password complexity can be set through:

- `minclass` - The minimum number of classes of characters required in a new password. (digits, uppercase, lowercase, others). e.g. `minclass = 4` requires digits, uppercase, lower case, and special characters.
- `dcredit` - The maximum credit for having digits in the new password. If less than `0` it is the minimum number of digits in the new password. e.g. `dcredit = -1` requires at least one digit
- `ucredit` - The maximum credit for having uppercase characters in the new password. If less than `0` it is the minimum number of uppercase characters in the new password. e.g. `ucredit = -1` requires at least one uppercase character
- `ocredit` - The maximum credit for having other characters in the new password. If less than `0` it is the minimum number of other characters in the new password. e.g. `ocredit = -1` requires at least one special character
- `lcredit` - The maximum credit for having lowercase characters in the new password. If less than `0` it is the minimum number of lowercase characters in the new password. e.g. `lcredit = -1` requires at least one lowercase character

#### **Rationale:**

Strong passwords protect systems from being hacked through brute force methods.

Requiring at least one non-alphabetic character increases the search space beyond pure dictionary words, which makes the resulting password harder to crack.

Forcing users to choose an excessively complex password, e.g. some combination of upper-case, lower-case, numbers, and special characters, has a negative impact. It places an extra burden on users and many will use predictable patterns (for example, a capital letter in the first position, followed by lowercase letters, then one or two numbers, and a “special character” at the end). Attackers know this, so dictionary attacks will often contain these common patterns and use the most common substitutions like, \$ for s, @ for a, 1 for l, 0 for o.

#### **Impact:**

Passwords that are too complex in nature make it harder for users to remember, leading to bad practices. In addition, composition requirements provide no defense against common attack types such as social engineering or insecure storage of passwords

## Audit:

Run the following command to verify:

- `dcredit`, `ucredit`, `lcredit`, and `ocredit` are not set to a value greater than 0
- Complexity conforms to local site policy:

```
# grep -Psi -- '^h*(minclass|[dulo]credit)\b' /etc/security/pwquality.conf  
/etc/security/pwquality.conf.d/*.conf
```

*Example output:*

```
/etc/security/pwquality.conf.d/50-pwcomplexity.conf:minclass = 3  
/etc/security/pwquality.conf.d/50-pwcomplexity.conf:ucredit = -2  
/etc/security/pwquality.conf.d/50-pwcomplexity.conf:lcredit = -2  
/etc/security/pwquality.conf.d/50-pwcomplexity.conf:dcredit = -1  
/etc/security/pwquality.conf.d/50-pwcomplexity.conf:ocredit = 0
```

The example represents a requirement of three character classes, with passwords requiring two upper case, two lower case, and one numeric character.

Run the following command to verify that module arguments in the configuration file(s) are not being overridden by arguments in `/etc/pam.d/common-password`:

```
grep -Psi --  
'^h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([^\#\n\r]+\h+)?(minclass=\d*|[dulo]credit=-?\d*)\b' /etc/pam.d/common-password
```

Nothing should be returned

## Note:

- settings should be configured in only **one** location for clarity
- Settings observe an order of precedence:
  - module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
  - settings in the `/etc/security/pwquality.conf` configuration file override settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory
  - settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory for clarity, convenience, and durability.

## Remediation:

Run the following command:

```
# grep -Pl --  
\bpam_pwquality\.so\h+([^\#\n\r]+[^\h+)?(minclass|[dulo]credit)\b'  
/usr/share/pam-configs/*
```

Edit any returned files and remove the minclass, dcredit, ucredit, lcredit, and ocredit arguments from the pam\_pwquality.so line(s)

Create or modify a file ending in .conf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line(s) to set complexity according to local site policy:

- minclass = \_N\_
- dcredit = \_N\_ # Value should be either 0 or a number proceeded by a minus (-) symbol
- ucredit = -1 # Value should be either 0 or a number proceeded by a minus (-) symbol
- ocredit = -1 # Value should be either 0 or a number proceeded by a minus (-) symbol
- lcredit = -1 # Value should be either 0 or a number proceeded by a minus (-) symbol

**Example 1 - Set minclass = 3:**

```
#!/usr/bin/env bash  
  
{  
    sed -ri 's/^s*minclass\s*/# &/' /etc/security/pwquality.conf  
    sed -ri 's/^s*[dulo]credit\s*/# &/' /etc/security/pwquality.conf  
    [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir  
    /etc/security/pwquality.conf.d/  
    printf '\n%s' "minclass = 3" > /etc/security/pwquality.conf.d/50-  
    pwcomplexity.conf  
}
```

**Example 2 - set dcredit = -1, ucredit = -1, and lcredit = -1:**

```
#!/usr/bin/env bash  
  
{  
    sed -ri 's/^s*minclass\s*/# &/' /etc/security/pwquality.conf  
    sed -ri 's/^s*[dulo]credit\s*/# &/' /etc/security/pwquality.conf  
    [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir  
    /etc/security/pwquality.conf.d/  
    printf '%s\n' "dcredit = -1" "ucredit = -1" "lcredit = -1" >  
    /etc/security/pwquality.conf.d/50-pwcomplexity.conf  
}
```

## **Default Value:**

minclass = 0

dcredit = 0

ucredit = 0

ocredit = 0

lcredit = 0

## **References:**

1. pam\_pwquality(8)
2. PWQUALITY.CONF(5)
3. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>
4. NIST SP 800-53 Rev. 5: IA-5

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

#### *5.3.3.2.4 Ensure password same consecutive characters is configured (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The `pwquality maxrepeat` option sets the maximum number of allowed same consecutive characters in a new password.

##### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

## Audit:

Run the following command to verify that the `maxrepeat` option is set to 3 or less, not 0, and follows local site policy:

```
# grep -Psi -- '^\\h*maxrepeat\\h*=\\h*[1-3]\\b' /etc/security/pwquality.conf  
/etc/security/pwquality.conf.d/*.*.conf
```

*Example output:*

```
/etc/security/pwquality.conf.d/50-pwrepeat.conf:maxrepeat = 3
```

Verify returned value(s) are 3 or less, not 0, and meet local site policy

Run the following command to verify that `maxrepeat` is not set, is 3 or less, not 0, and conforms to local site policy:

```
grep -Psi --  
'^\\h*password\\h+(requisite|required|sufficient)\\h+pam_pwquality\\.so\\h+([^\n\r]+\\h+)?maxrepeat\\h*=\\h*(0|[4-9]| [1-9] [0-9]+)\\b' /etc/pam.d/common-password
```

```
Nothing should be returned
```

## Note:

- settings should be configured in only **one** location for clarity
- Settings observe an order of precedence:
  - module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
  - settings in the `/etc/security/pwquality.conf` configuration file override settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory
  - settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory for clarity, convenience, and durability.

## **Remediation:**

Create or modify a file ending in .conf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line to set maxrepeat to 3 or less and not 0. Ensure setting conforms to local site policy:

*Example:*

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

{
    sed -ri 's/^s*maxrepeat\s*/# &/' /etc/security/pwquality.conf
    [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir
/etc/security/pwquality.conf.d/
    printf '\n%s' "maxrepeat = 3" > /etc/security/pwquality.conf.d/50-
pwrepeat.conf
}
```

Run the following command:

```
# grep -Pl -- '\bpam_pwquality\.so\h+([^\#\n\r]+\h+)\?maxrepeat\b'
/usr/share/pam-configs/*
```

Edit any returned files and remove the maxrepeat argument from the pam\_pwquality.so line(s):

## **Default Value:**

maxrepeat = 0

## **References:**

1. NIST SP 800-53 Rev. 5: IA-5

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

### *5.3.3.2.5 Ensure password maximum sequential characters is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `pwquality maxsequence` option sets the maximum length of monotonic character sequences in the new password. Examples of such sequence are `12345` or `fedcb`. The check is disabled if the value is `0`.

**Note:** Most such passwords will not pass the simplicity check unless the sequence is only a minor part of the password.

#### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

## Audit:

Run the following command to verify that the `maxsequence` option is set to 3 or less, not 0, and follows local site policy:

```
# grep -Psi -- '^h*maxsequence\h*=\h*[1-3]\b' /etc/security/pwquality.conf  
/etc/security/pwquality.conf.d/*.*conf
```

*Example output:*

```
/etc/security/pwquality.conf.d/50-pwmaxsequence.conf:maxsequence = 3
```

Verify returned value(s) are 3 or less, not 0, and meet local site policy

Run the following command to verify that `maxsequence` is not set, is 3 or less, not 0, and conforms to local site policy:

```
grep -Psi --  
'^h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([^\#\n\r]+\h+)\?maxsequence\h*=\h*(0|[4-9]|1-9)[0-9]+)\b' /etc/pam.d/common-password
```

```
Nothing should be returned
```

## Note:

- settings should be configured in only **one** location for clarity
- Settings observe an order of precedence:
  - module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
  - settings in the `/etc/security/pwquality.conf` configuration file override settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory
  - settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory for clarity, convenience, and durability.

## **Remediation:**

Create or modify a file ending in .conf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line to set maxsequence to 3 or less and not 0. Ensure setting conforms to local site policy:

*Example:*

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

{
    sed -ri 's/^s*maxsequence\s*/# &/' /etc/security/pwquality.conf
    [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir
/etc/security/pwquality.conf.d/
    printf '\n%s' "maxsequence = 3" > /etc/security/pwquality.conf.d/50-
pwmaxsequence.conf
}
```

Run the following command:

```
# grep -Pl -- '\bpam_pwquality\.so\h+([^\#\n\r]+\h+)\?maxsequence\b'
/usr/share/pam-configs/*
```

Edit any returned files and remove the maxsequence argument from the pam\_pwquality.so line(s):

## **Default Value:**

maxsequence = 0

## **References:**

1. NIST SP 800-53 Rev. 5: IA-5

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

### *5.3.3.2.6 Ensure password dictionary check is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `pwquality dictcheck` option sets whether to check for the words from the `cracklib` dictionary.

#### **Rationale:**

If the operating system allows the user to select passwords based on dictionary words, this increases the chances of password compromise by increasing the opportunity for successful guesses, and brute-force attacks.

## Audit:

Run the following command to verify that the `dictcheck` option is not set to 0 (disabled) in a `pwquality` configuration file:

```
# grep -Psi -- '^h*dictcheck\h*=\h*0\b' /etc/security/pwquality.conf  
/etc/security/pwquality.conf.d/*.*.conf  
  
Nothing should be returned
```

Run the following command to verify that the `dictcheck` option is not set to 0 (disabled) as a module argument in a PAM file:

```
# grep -Psi --  
'^h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([^\#\n\r]+\h+)\?dictcheck\h*=\h*0\b' /etc/pam.d/common-password  
  
Nothing should be returned
```

## Note:

- Settings observe an order of precedence:
  - module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
  - settings in the `/etc/security/pwquality.conf` configuration file override settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory
  - settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory for clarity, convenience, and durability.

## Remediation:

Edit any file ending in `.conf` in the `/etc/security/pwquality.conf.d/` directory and/or the file `/etc/security/pwquality.conf` and comment out or remove any instance of `dictcheck = 0`:

### Example:

```
# sed -ri 's/^s*dictcheck\s*/# &/' /etc/security/pwquality.conf  
/etc/security/pwquality.conf.d/*.*.conf
```

Run the following command:

```
# grep -Pl -- '\bpam_pwquality\.so\h+([^\#\n\r]+\h+)\?dictcheck\b'  
/usr/share/pam-configs/*
```

Edit any returned files and remove the `dictcheck` argument from the `pam_pwquality.so` line(s)

**Default Value:**

dictcheck = 1

**References:**

1. NIST SP 800-53 Rev. 5: IA-5

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

### *5.3.3.2.7 Ensure password quality checking is enforced (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `pam_pwquality` module can be configured to either reject a password if it fails the checks, or only print a warning.

This is configured by setting the `enforcing=<N>` argument. If nonzero, a password will be rejected if it fails the checks, otherwise only a warning message will be provided.

This setting applies only to the `pam_pwquality` module and possibly other applications that explicitly change their behavior based on it. It does not affect `pwmake(1)` and `pwscore(1)`.

#### **Rationale:**

Strong passwords help protect systems from password attacks. Types of password attacks include dictionary attacks, which attempt to use common words and phrases, and brute force attacks, which try every possible combination of characters. Also attackers may try to obtain the account database so they can use tools to discover the accounts and passwords.

#### **Audit:**

Run the following command to verify that `enforcing=0` has not been set in a `pwquality` configuration file:

```
# grep -PHsi -- '^\\h*enforcing\\h*=\\h*0\\b' /etc/security/pwquality.conf  
/etc/security/pwquality.conf.d/*.*.conf
```

Nothing should be returned

Run the following command to verify that the `enforcing=0` argument has not been set on the `pam_pwquality` module:

```
# grep -PHsi --  
'^\\h*password\\h+[^#\\n\\r]+\\h+pam_pwquality\\.so\\h+([^\n\\r]+\\h+) ?enforcing=0\\b'  
/etc/pam.d/common-password
```

Nothing should be returned

## **Remediation:**

Run the following command:

```
# grep -Pl -- '\bpam_pwquality\.so\b+([^\#\n\r]+\b+)?enforcing=0\b' /usr/share/pam-configs/*
```

Edit any returned files and remove the `enforcing=0` argument from the `pam_pwquality.so` line(s)

Edit `/etc/security/pwquality.conf` and all files ending in `.conf` in the `/etc/security/pwquality.conf.d/` directory and remove or comment out any line containing the `enforcing = 0` argument:

*Example:*

```
# sed -ri 's/^s*enforcing\s*=\\s*0/# &/' /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

## **Default Value:**

`enforcing=1`

## **References:**

1. `pam_pwquality(8)`
2. `PWQUALITY.CONF(5)`
3. NIST SP 800-53 Rev. 5: IA-5

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

### *5.3.3.2.8 Ensure password quality is enforced for the root user (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

If the `pwquality enforce_for_root` option is enabled, the module will return error on failed check even if the user changing the password is root.

This option is off by default which means that just the message about the failed check is printed but root can change the password anyway.

**Note:** The root is not asked for an old password so the checks that compare the old and new password are not performed.

#### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

## Audit:

Run the following command to verify that the `enforce_for_root` option is enabled in a `pwquality` configuration file:

```
# grep -Psi -- '^h*enforce_for_root\b' /etc/security/pwquality.conf  
/etc/security/pwquality.conf.d/*.conf
```

*Example output:*

```
/etc/security/pwquality.conf.d/50-pwroot.conf:enforce_for_root
```

## Note:

- Settings observe an order of precedence:
  - module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
  - settings in the `/etc/security/pwquality.conf` configuration file override settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory
  - settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory for clarity, convenience, and durability.

## Remediation:

Edit or add the following line in a `*.conf` file in `/etc/security/pwquality.conf.d` or in `/etc/security/pwquality.conf`:

*Example:*

```
#!/usr/bin/env bash  
  
{  
    [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir  
    /etc/security/pwquality.conf.d/  
    printf '\n%s\n' "enforce_for_root" > /etc/security/pwquality.conf.d/50-  
    pwroot.conf  
}
```

## Default Value:

disabled

## References:

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

### 5.3.3.3 Configure pam\_pwhistory module

pam\_pwhistory - PAM module to remember last passwords

pam\_history.so module - This module saves the last passwords for each user in order to force password change history and keep the user from alternating between the same password too frequently.

This module does not work together with kerberos. In general, it does not make much sense to use this module in conjunction with NIS or LDAP, since the old passwords are stored on the local machine and are not available on another machine for password history checking.

Options:

- debug - Turns on debugging via syslog(3).
- use\_authok - When password changing enforce the module to use the new password provided by a previously stacked password module (this is used in the example of the stacking of the pam\_passwdqc module documented below).
- enforce\_for\_root - If this option is set, the check is enforced for root, too.
- remember=<N> - The last <N> passwords for each user are saved. The default is 10. Value of 0 makes the module to keep the existing contents of the opasswd file unchanged.
- retry=<N> - Prompt user at most <N> times before returning with error. The default is 1.
- authok\_type=<STRING> - See pam\_get\_authok(3) for more details.

Examples:

An example password section would be:

```
#%PAM-1.0
password required pam_pwhistory.so
password required pam_unix.so           use_authok
```

In combination with pam\_passwdqc:

```
#%PAM-1.0
password required pam_passwdqc.so    config=/etc/passwdqc.conf
password required pam_pwhistory.so   use_authok
password required pam_unix.so        use_authok
```

### *5.3.3.3.1 Ensure password history remember is configured (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. The number of passwords remembered is set via the `remember` argument value in set for the `pam_pwhistory` module.

- `remember=<N>` - `<N>` is the number of old passwords to remember

#### **Rationale:**

Requiring users not to reuse their passwords make it less likely that an attacker will be able to guess the password or use a compromised password.

**Note:** These change only apply to accounts configured on the local system.

#### **Audit:**

Run the following command and verify:

- The `pwhistory` line in `/etc/pam.d/common-password` includes `remember=<N>`
- The value of `<N>` is 24 or more
- The value meets local site policy

```
# grep -Psi --  
'^h*password\h+[^#\n\r]+\h+pam_pwhistory\.so\h+([^\#\n\r]+\h+)?remember=\d+\b'  
/etc/pam.d/common-password
```

Output should be similar to:

```
password    requisite    pam_pwhistory.so remember=24 enforce_for_root  
try_first_pass use_authok
```

## **Remediation:**

Run the following command:

```
# awk '/Password-Type:/ { f = 1;next } /-Type:/ { f = 0 } f {if (/pam_pwhistory\.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files and edit or add the `remember=` argument, with a value of 24 or more, that meets local site policy to the `pam_pwhistory` line in the Password section:

*Example File:*

```
Name: pwhistory password history checking
Default: yes
Priority: 1024
Password-Type: Primary
Password:
    requisite    pam_pwhistory.so remember=24 enforce_for_root try_first_pass
use_authtok # <- **ensure line includes remember=<N>**
```

Run the following command to update the files in the `/etc/pam.d/` directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

*Example:*

```
# pam-auth-update --enable pwhistory
```

## **References:**

1. NIST SP 800-53 Rev. 5: IA-5(1)

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.004		

### *5.3.3.3.2 Ensure password history is enforced for the root user (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

If the `pwhistory enforce_for_root` option is enabled, the module will enforce password history for the root user as well

#### **Rationale:**

Requiring users not to reuse their passwords make it less likely that an attacker will be able to guess the password or use a compromised password

**Note:** These changes only apply to accounts configured on the local system.

#### **Audit:**

Run the following command to verify that the `enforce_for_root` argument exists on the `pwhistory` line in `/etc/pam.d/common-password`:

```
# grep -Psi -- '^h*password\h+[^#\n\r]+\h+pam_pwhistory\.so\h+([^\#\n\r]+\h+)?enforce_for_root\b' /etc/pam.d/common-password
```

Output should be similar to:

```
password    requisite    pam_pwhistory.so remember=24 enforce_for_root
try_first_pass use_authok
```

## **Remediation:**

Run the following command:

```
# awk '/Password-Type:/ { f = 1;next } /-Type:/ { f = 0 } f {if (/pam_pwhistory\.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files and add the `enforce_for_root` argument to the `pam_pwhistory` line in the `Password` section:

*Example File:*

```
Name: pwhistory password history checking
Default: yes
Priority: 1024
Password-Type: Primary
Password:
    requisite    pam_pwhistory.so remember=24 enforce_for_root try_first_pass
use_authtok # <- **ensure line includes enforce_for_root**
```

Run the following command to update the files in the `/etc/pam.d/` directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

*Example:*

```
# pam-auth-update --enable pwhistory
```

**Default Value:**

disabled

**References:**

1. NIST SP 800-53 Rev. 5: IA-5

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

### *5.3.3.3.3 Ensure pam\_pwhistory includes use\_authok (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

`use_authok` - When password changing enforce the module to set the new password to the one provided by a previously stacked password module

#### **Rationale:**

`use_authok` allows multiple pam modules to confirm a new password before it is accepted.

#### **Audit:**

Run the following command to verify that the `use_authok` argument exists on the `pwhistory` line in `/etc/pam.d/common-password`:

```
# grep -Psi --  
'^h*password\h+[^#\n\r]+\h+pam_pwhistory\.so\h+([^\#\n\r]+\h+)\?use_authok\b'  
/etc/pam.d/common-password
```

Output should be similar to:

```
password    requisite    pam_pwhistory.so remember=24 enforce_for_root  
try_first_pass use_authok
```

## **Remediation:**

Edit any returned files and add the `use_authok` argument to the `pam_pwhistory` line in the `Password` section:

### *Example File:*

```
Name: pwhistory password history checking
Default: yes
Priority: 1024
Password-Type: Primary
Password:
    requisite    pam_pwhistory.so remember=24 enforce_for_root try_first_pass
use_authok # <- **ensure line includes use_authok**
```

Run the following command to update the files in the `/etc/pam.d/` directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

### *Example:*

```
# pam-auth-update --enable pwhistory
```

## **References:**

1. NIST SP 800-53 Rev. 5: IA-5

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 Encrypt Sensitive Data at Rest</b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>16.4 Encrypt or Hash all Authentication Credentials</b> 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

#### **5.3.3.4 Configure pam\_unix module**

The `pam_unix.so` module is the standard Unix authentication module. It uses standard calls from the system's libraries to retrieve and set account information as well as authentication. Usually this is obtained from the `/etc/passwd` and the `/etc/shadow` file as well if shadow is enabled.

### *5.3.3.4.1 Ensure pam\_unix does not include nullok (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `nullok` argument overrides the default action of `pam_unix.so` to not permit the user access to a service if their official password is blank.

#### **Rationale:**

Using a strong password is essential to helping protect personal and sensitive information from unauthorized access

#### **Audit:**

Run the following command to verify that the `nullok` argument is not set on the `pam_unix.so` module:

```
# grep -PH -- '^\\h*^\\h*[^#\\n\\r]+\\h+pam_unix\\.so\\b' /etc/pam.d/common-{password,auth,account,session,session-noninteractive} | grep -Pv -- '\bnullok\\b'
```

Output should be similar to:

```
/etc/pam.d/common-password:password    [success=1 default=ignore]
pam_unix.so obscure use_authok try_first_pass yescrypt
/etc/pam.d/common-auth:auth    [success=2 default=ignore]    pam_unix.so
try_first_pass
/etc/pam.d/common-account:account    [success=1 new_authok_reqd=done
default=ignore]    pam_unix.so
/etc/pam.d/common-session:session    required    pam_unix.so
/etc/pam.d/common-session-noninteractive:session    required    pam_unix.so
```

## **Remediation:**

Run the following command:

```
# grep -PH -- '^\\h*([^\n\r]+\h+)?pam_unix\\.so\\h+([^\n\r]+\h+)?nullok\\b' /usr/share/pam-configs/*
```

Edit any files returned and remove the `nulllok` argument for the `pam_unix` lines

*Example File:*

```
Name: Unix authentication
Default: yes
Priority: 256
Auth-Type: Primary
Auth:
    [success=end default=ignore]      pam_unix.so try_first_pass # <-
**ensure line does not include nullok nullok**
Auth-Initial:
    [success=end default=ignore]      pam_unix.so # <- **ensure line does
not include nullok nullok**
Account-Type: Primary
Account:
    [success=end new_authtok_reqd=done default=ignore]      pam_unix.so
Account-Initial:
    [success=end new_authtok_reqd=done default=ignore]      pam_unix.so
Session-Type: Additional
Session:
    required      pam_unix.so
Session-Initial:
    required      pam_unix.so
Password-Type: Primary
Password:
    [success=end default=ignore]      pam_unix.so obscure use_authtok
try_first_pass yescript
Password-Initial:
    [success=end default=ignore]      pam_unix.so obscure yescript
```

Run the following command to update the files in the `/etc/pam.d/` directory:

```
# pam-auth-update --enable <EDITED_PROFILE_NAME>
```

*Example:*

```
# pam-auth-update --enable unix
```

**Note:** If custom files are being used, the corresponding files in `/etc/pam.d/` would need to be edited directly, and the `pam-auth-update --enable <EDITED_PROFILE_NAME>` command skipped

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.</p>	●	●	●
v7	<p><b>4.4 Use Unique Passwords</b> 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>		●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1110, T1110.002	TA0006	M1041

### *5.3.3.4.2 Ensure pam\_unix does not include remember (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `remember=n` argument saves the last n passwords for each user in `/etc/security/opasswd` in order to force password change history and keep the user from alternating between the same password too frequently. The MD5 password hash algorithm is used for storing the old passwords. Instead of this option the `pam_pwhistory` module should be used. The `pam_pwhistory` module saves the last n passwords for each user in `/etc/security/opasswd` using the password hash algorithm set on the `pam_unix` module. This allows for the `yescrypt` or `sha512` hash algorithm to be used.

#### **Rationale:**

The `remember=n` argument should be removed to ensure a strong password hashing algorithm is being used. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local user's old passwords stored in `/etc/security/opasswd`.

#### **Audit:**

Run the following command to verify that the `remember` argument is not set on the `pam_unix.so` module:

```
# grep -PH -- '^h*^h*[^\n\r]+\h+pam_unix\.so\b' /etc/pam.d/common-{password,auth,account,session,session-noninteractive} | grep -Pv -- '\bremember=\d+\b'
```

Output should be similar to:

```
/etc/pam.d/common-password:password    [success=1 default=ignore]
pam_unix.so obscure yescrypt
/etc/pam.d/common-auth:auth    [success=1 default=ignore]    pam_unix.so
/etc/pam.d/common-account:account    [success=1 new_authtok_reqd=done
default=ignore]    pam_unix.so
/etc/pam.d/common-session:session    required    pam_unix.so
/etc/pam.d/common-session-noninteractive:session    required    pam_unix.so
```

## Remediation:

Run the following command:

```
# grep -PH -- '^\\h*([^\#\\n\\r]+\\h+)?pam_unix\\.so\\h+([^\#\\n\\r]+\\h+)?remember\\b' /usr/share/pam-configs/*
```

Edit any files returned and remove the `remember=_<N>_` argument for the `pam_unix` lines  
*Example output:*

```
[success=end default=ignore] pam_unix.so obscure use_authok try_first_pass  
yescrypt remember=5 # **<- remove remember=<N>**  
[success=end default=ignore] pam_unix.so obscure yescrypt remember=5 # **<-  
remove remember=<N>**
```

Run the following command to update the files in the `/etc/pam.d/` directory:

```
# pam-auth-update --enable <EDITED_PROFILE_NAME>
```

*Example:*

```
# pam-auth-update --enable unix
```

**Note:** If custom files are being used, the corresponding files in `/etc/pam.d/` would need to be edited directly, and the `pam-auth-update --enable <EDITED_PROFILE_NAME>` command skipped

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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, T1110, T1110.002	TA0006	M1041

### *5.3.3.4.3 Ensure pam\_unix includes a strong password hashing algorithm (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.

The `pam_unix` module can be configured to use one of the following hashing algorithms for user's passwords:

- `md5` - When a user changes their password next, encrypt it with the `MD5` algorithm.
- `bigrrypt` - When a user changes their password next, encrypt it with the `DEC C2` algorithm.
- `sha256` - When a user changes their password next, encrypt it with the `SHA256` algorithm. The `SHA256` algorithm must be supported by the `crypt(3)` function.
- `sha512` - When a user changes their password next, encrypt it with the `SHA512` algorithm. The `SHA512` algorithm must be supported by the `crypt(3)` function.
- `blowfish` - When a user changes their password next, encrypt it with the `blowfish` algorithm. The `blowfish` algorithm must be supported by the `crypt(3)` function.
- `gost_yescrypt` - When a user changes their password next, encrypt it with the `gost-yescrypt` algorithm. The `gost-yescrypt` algorithm must be supported by the `crypt(3)` function.
- `yescrypt` - When a user changes their password next, encrypt it with the `yescrypt` algorithm. The `yescrypt` algorithm must be supported by the `crypt(3)` function.

#### **Rationale:**

The `SHA-512` and `yescrypt` algorithms provide a stronger hash than other algorithms used by Linux for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local user passwords.

**Note:** These changes only apply to the local system.

## Audit:

Run the following command to verify that a strong password hashing algorithm is set on the pam\_unix.so module:

```
# grep -PH --  
'^h*password\h+([^\#\n\r]+)\h+pam_unix\.so\h+([^\#\n\r]+\h+)?(sha512|yescrypt)  
\b' /etc/pam.d/common-password
```

Output should be similar to:

```
/etc/pam.d/common-password:password [success=1 default=ignore]  
pam_unix.so obscure use_authok try_first_pass yescrypt
```

Verify that the line(s) include either sha512 - **OR** - yescrypt

## **Remediation:**

Run the following command:

```
# awk '/Password-Type:/ { f = 1;next } /-Type:/ { f = 0 } f {if (/pam_unix\.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files and edit or add a strong hashing algorithm, either sha512 or yescript, that meets local site policy to the `pam_unix` lines in the `Password` section:

*Example File:*

```
Name: Unix authentication
Default: yes
Priority: 256
Auth-Type: Primary # <- Start of "Auth" section
Auth:
    [success=end default=ignore]      pam_unix.so try_first_pass
Auth-Initial:
    [success=end default=ignore]      pam_unix.so
Account-Type: Primary # <- Start of "Account" section
Account:
    [success=end new_authtok_reqd=done default=ignore]      pam_unix.so
Account-Initial:
    [success=end new_authtok_reqd=done default=ignore]      pam_unix.so
Session-Type: Additional # <- Start of "Session" section
Session:
    required      pam_unix.so
Session-Initial:
    required      pam_unix.so
Password-Type: Primary # <- Start of "Password" section
Password:
    [success=end default=ignore]      pam_unix.so obscure use_authok
try_first_pass yescript # <- **ensure hashing algorithm is either sha512 or
yescript**
Password-Initial:
    [success=end default=ignore]      pam_unix.so obscure yescript # <-
**ensure hashing algorithm is either sha512 or yescript**
```

Run the following command to update the files in the `/etc/pam.d/` directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

*Example:*

```
# pam-auth-update --enable unix
```

## **References:**

1. NIST SP 800-53 Rev. 5: IA-5

## **Additional Information:**

The following command may be used to expire all non-system user ID's immediately and force them to change their passwords on next login. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# awk -F: '($3<"$(awk '/^UID_MIN/{print $2}' /etc/login.defs)" && $1 != "nobody") { print $1 }' /etc/passwd | xargs -n 1 chage -d 0
```

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 Encrypt Sensitive Data at Rest</b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>16.4 Encrypt or Hash all Authentication Credentials</b> 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

#### *5.3.3.4.4 Ensure pam\_unix includes use\_authok (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

`use_authok` - When password changing enforce the module to set the new password to the one provided by a previously stacked password module

##### **Rationale:**

`use_authok` allows multiple pam modules to confirm a new password before it is accepted.

##### **Audit:**

Run the following command to verify that `use_authok` is set on the `pam_unix.so` module lines in the password stack:

```
# grep -PH --  
'^h*password\h+([^\#\n\r]+)\h+pam_unix\.so\h+([^\#\n\r]+\h+)?use_authok\b'  
/etc/pam.d/common-password
```

Output should be similar to:

```
/etc/pam.d/common-password:password    [success=1 default=ignore]  
pam_unix.so obscure use_authok try_first_pass yescrypt
```

Verify that the line(s) include `use_authok`

## **Remediation:**

Run the following command:

```
# awk '/Password-Type:/ { f = 1;next } /-Type:/ { f = 0 } f {if (/pam_unix\.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files add `use_authok` to the `pam_unix` line in the `Password` section under `Password:` subsection:

**Note:** The if the file's `Password` section includes a `Password-Initial:` subsection, `use_authok` should not be added to the `pam_unix` line in the `Password-Initial:` subsection

*Example File:*

```
Name: Unix authentication
Default: yes
Priority: 256
Auth-Type: Primary # <- Start of "Auth" section
Auth:
    [success=end default=ignore]      pam_unix.so try_first_pass
Auth-Initial:
    [success=end default=ignore]      pam_unix.so
Account-Type: Primary # <- Start of "Account" section
Account:
    [success=end new_authok_reqd=done default=ignore]      pam_unix.so
Account-Initial:
    [success=end new_authok_reqd=done default=ignore]      pam_unix.so
Session-Type: Additional # <- Start of "Session" section
Session:
    required      pam_unix.so
Session-Initial:
    required      pam_unix.so
Password-Type: Primary # <- Start of "Password" section
Password:
    [success=end default=ignore]      pam_unix.so obscure use_authok
try_first_pass yescript # <- **ensure line includes use_authok**
Password-Initial:
    [success=end default=ignore]      pam_unix.so obscure yescript # <-
**Password-Initial: subsection does not include use_authok
```

Run the following command to update the files in the `/etc/pam.d/` directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

*Example:*

```
# pam-auth-update --enable unix
```

## **References:**

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.11 Encrypt Sensitive Data at Rest</b>            Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.</p>	●	●	●
v7	<p><b>16.4 Encrypt or Hash all Authentication Credentials</b>            Encrypt or hash with a salt all authentication credentials when stored.</p>	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1110, T1110.002	TA0006	M1041

## **5.4 User Accounts and Environment**

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

### **5.4.1 Configure shadow password suite parameters**

While a majority of the password control parameters have been moved to PAM, some parameters are still available through the shadow password suite. Any changes made to `/etc/login.defs` will only be applied if the `usermod` command is used. If user IDs are added a different way, use the `chage` command to effect changes to individual user IDs.

### *5.4.1.1 Ensure password expiration is configured (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.

`PASS_MAX_DAYS <N>` - The maximum number of days a password may be used. If the password is older than this, a password change will be forced. If not specified, -1 will be assumed (which disables the restriction).

#### **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.

We recommend a yearly password change. This is primarily because for all their good intentions users will share credentials across accounts. Therefore, even if a breach is publicly identified, the user may not see this notification, or forget they have an account on that site. This could leave a shared credential vulnerable indefinitely. Having an organizational policy of a 1-year (annual) password expiration is a reasonable compromise to mitigate this with minimal user burden.

## **Impact:**

The password expiration must be greater than the minimum days between password changes or users will be unable to change their password.

Excessive password expiration requirements do more harm than good, because these requirements make users select predictable passwords, composed of sequential words and numbers that are closely related to each other. In these cases, the next password can be predicted based on the previous one (incrementing a number used in the password for example). Also, password expiration requirements offer no containment benefits because attackers will often use credentials as soon as they compromise them. Instead, immediate password changes should be based on key events including, but not limited to:

- Indication of compromise
- Change of user roles
- When a user leaves the organization.

Not only does changing passwords every few weeks or months frustrate the user, it's been suggested that it does more harm than good, because it could lead to bad practices by the user such as adding a character to the end of their existing password.

## **Audit:**

Run the following command and verify `PASS_MAX_DAYS` is set to 365 days or less and conforms to local site policy:

```
# grep -Pi -- '^h*PASS_MAX_DAYS\h+\d+\b' /etc/login.defs
```

*Example output:*

```
PASS_MAX_DAYS 365
```

Run the following command and Review list of users and `PASS_MAX_DAYS`s to verify that all users `PASS_MAX_DAYS` conforms to site policy (no more than 365 days):

Run the following command to verify all passwords have a `PASS_MAX_DAYS` of 365 days or less and greater than 0 days:

```
# awk -F: '($2~/^\$/ {if($5 > 365 || $5 < 1)print "User: " $1 " PASS_MAX_DAYS: " $5}' /etc/shadow
```

Nothing 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>
```

Edit `/etc/login.defs` and set `PASS_MAX_DAYS` to a value greater than 0 that follows local site policy:

*Example:*

```
PASS_MAX_DAYS 365
```

Run the following command to modify user parameters for all users with a password set to a maximum age no greater than 356 or less than 1 that follows local site policy:

```
# chage --maxdays <N> <user>
```

*Example:*

```
# awk -F: '($2~/^\$.[^\$/]{5}\$/) {if($5 > 365 || $5 < 1)system ("chage --maxdays 365\n\"$1")}' /etc/shadow
```

## **Default Value:**

`PASS_MAX_DAYS 99999`

## **References:**

1. CIS Password Policy Guide
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## **Additional Information:**

A value of -1 will disable password expiration.

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.001, T1110.002, T1110.003, T1110.004		

### *5.4.1.2 Ensure minimum password age is configured (Manual)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The minimum password age determines the number of days that you must use a password before you can change it.

`PASS_MIN_DAYS <N>` - The minimum number of days allowed between password changes. Any password changes attempted sooner than this will be rejected. If not specified, 0 will be assumed (which disables the restriction).

#### **Rationale:**

Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old, potentially compromised passwords, may cause a security breach.

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

#### **Impact:**

By enforcing a minimum password age, a user will be unable to change their password if they observe a potential compromise of their password, e.g. "shoulder surfing", during the time defined by minimum password age. In this event the user should follow local site policy to report a compromised password.

If a users password is set by other personnel as a procedure in dealing with a lost or expired password, the user should be forced to update this "set" password with their own password. e.g. force "change at next logon".

If it is not possible to have a user set their own password immediately, and this recommendation or local site procedure may cause a user to continue using a third party generated password, `PASS_MIN_DAYS` for the effected user should be temporally changed to 0, to allow a user to change their password immediately.

For applications where the user is not using the password at console, the ability to "change at next logon" may be limited. This may cause a user to continue to use a password created by other personnel.

## Audit:

Run the following command to verify that `PASS_MIN_AGE` is set to a value greater than 0 and follows local site policy:

```
# grep -Pi -- '^h*PASS_MIN_DAYS\h+\d+\b' /etc/login.defs
```

*Example output:*

```
PASS_MIN_DAYS 1
```

Run the following command to verify all passwords have a `PASS_MIN_AGE` greater than 0:

```
# awk -F: '$2~/^\$./ {if($4 < 1)print "User: " $1 " PASS_MIN_DAYS: " $4}' /etc/shadow
```

Nothing should be returned

## Remediation:

Edit `/etc/login.defs` and set `PASS_MIN_DAYS` to a value greater than 0 that follows local site policy:

*Example:*

```
PASS_MIN_DAYS 1
```

Run the following command to modify user parameters for all users with a password set to a minimum age greater than zero that follows local site policy:

```
# chage --mindays <N> <user>
```

*Example:*

```
# awk -F: '$2~/^\$./ {if($4 < 1)system ("chage --mindays 1 " $1)}' /etc/shadow
```

## Default Value:

`PASS_MIN_DAYS 0`

## References:

1. CIS Password Policy Guide

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.2 Use Unique Passwords</b>            Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.</p>	●	●	●
v7	<p><b>4.4 Use Unique Passwords</b>            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>		●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.004	TA0006	M1027

### *5.4.1.3 Ensure password expiration warning days is configured (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.

`PASS_WARN_AGE <N>` - The number of days warning given before a password expires. A zero means warning is given only upon the day of expiration, a negative value means no warning is given. If not specified, no warning will be provided.

#### **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` is 7 or more and follows local site policy:

```
# grep -Pi -- '^h*PASS_WARN_AGE\h+\d+\b' /etc/login.defs
```

#### *Example output:*

```
PASS_WARN_AGE 7
```

Run the following command to verify all passwords have a `PASS_WARN_AGE` of 7 or more:

```
# awk -F: '($2~/^\$/){if($6<7)print "User: " $1 " PASS_WARN_AGE: " $6}' /etc/shadow
```

Nothing should be returned

## **Remediation:**

Edit `/etc/login.defs` and set `PASS_WARN_AGE` to a value of 7 or more that follows local site policy:

*Example:*

```
PASS_WARN_AGE 7
```

Run the following command to modify user parameters for all users with a password set to a minimum warning to 7 or more days that follows local site policy:

```
# chage --warndays <N> <user>
```

*Example:*

```
# awk -F: '$2~/^\$.*\$/ {if($6 < 7)system ("chage --warndays 7 " $1)}'  
/etc/shadow
```

## **Default Value:**

`PASS_WARN_AGE 7`

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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	TA0006	M1027

#### *5.4.1.4 Ensure strong password hashing algorithm is configured (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.

`ENCRYPT_METHOD (string)` - This defines the system default encryption algorithm for encrypting passwords (if no algorithm are specified on the command line). It can take one of these values:

- `MD5` - MD5-based algorithm will be used for encrypting password
- `SHA256` - SHA256-based algorithm will be used for encrypting password
- `SHA512` - SHA512-based algorithm will be used for encrypting password
- `BCRYPT` - BCRYPT-based algorithm will be used for encrypting password
- `YESCRYPT` - YESCRYPT-based algorithm will be used for encrypting password
- `DES` - DES-based algorithm will be used for encrypting password (default)

##### **Note:**

- This parameter overrides the deprecated `MD5_CRYPT_ENAB` variable.
- This parameter will only affect the generation of group passwords.
- The generation of user passwords is done by PAM and subject to the PAM configuration.
- It is recommended to set this variable consistently with the PAM configuration.

##### **Rationale:**

The `SHA-512` and `yescrypt` algorithms provide a stronger hash than other algorithms used by Linux for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local group passwords.

## Audit:

Run the following command to verify the hashing algorithm is sha512 or yescrypt in /etc/login.defs:

```
# grep -Pi -- '^h*ENCRYPT_METHOD\h+(SHA512|yescrypt)\b' /etc/login.defs
```

*Example output:*

```
ENCRYPT_METHOD SHA512
- OR -
ENCRYPT_METHOD YESCRYPT
```

## Remediation:

Edit /etc/login.defs and set the ENCRYPT\_METHOD to SHA512 or YESCRYPT:

```
ENCRYPT_METHOD <HASHING_ALGORITHM>
```

*Example:*

```
ENCRYPT_METHOD YESCRYPT
```

## Note:

- This only effects local groups' passwords created after updating the file to use sha512 or yescript.
- If it is determined that the password algorithm being used is not sha512 or yescript, once it is changed, it is recommended that all group passwords be updated to use the stronger hashing algorithm.
- It is recommended that the chosen hashing algorithm is consistent across /etc/login.defs and the PAM configuration

## Default Value:

ENCRYPT\_METHOD SHA512

## References:

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.11 Encrypt Sensitive Data at Rest</b>            Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.</p>	●	●	●
v7	<p><b>16.4 Encrypt or Hash all Authentication Credentials</b>            Encrypt or hash with a salt all authentication credentials when stored.</p>	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1110, T1110.002	TA0006	M1041

### *5.4.1.5 Ensure inactive password lock is configured (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.

`INACTIVE` - Defines the number of days after the password exceeded its maximum age where the user is expected to replace this password.

The value is stored in the shadow password file. An input of `0` will disable an expired password with no delay. An input of `-1` will blank the respective field in the shadow password file.

#### **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 45 days):

```
# useradd -D | grep INACTIVE  
INACTIVE=45
```

Verify all users with a password have Password inactive no more than 45 days after password expires

Verify all users with a password have Password inactive no more than 45 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 45 days):

```
# awk -F: '($2~/^\$/ || $2~/^!/) {if($7 > 45 || $7 < 0)print "User: " $1 " INACTIVE: " $7}' /etc/shadow
```

Nothing should be returned

## **Remediation:**

Run the following command to set the default password inactivity period to 45 days or less that meets local site policy:

```
# useradd -D -f <N>
```

*Example:*

```
# useradd -D -f 45
```

Run the following command to modify user parameters for all users with a password set to an inactive age of 45 days or less that follows local site policy:

```
# chage --inactive <N> <user>
```

*Example:*

```
# awk -F: '($2~/^\$/ || $2~/.+\$/){if($7 > 45 || $7 < 0)system ("chage --inactive 45\n\"$1\"")}' /etc/shadow
```

## **Default Value:**

INACTIVE=-1

## **References:**

1. CIS Password Policy Guide

## **Additional Information:**

A value of -1 would disable this setting.

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	<b>4.4 Use Unique Passwords</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1078, T1078.002, T1078.003	TA0001	M1027

### *5.4.1.6 Ensure all users last password change date is in the past (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

All users should have a password change date in the past.

#### **Rationale:**

If a user's recorded password change date is in the future, then they could bypass any set password expiration.

#### **Audit:**

Run the following command and verify nothing is returned

```
{  
    while IFS= read -r l_user; do  
        l_change=$(date -d "$(chage --list $l_user | grep '^Last password  
change' | cut -d: -f2 | grep -v 'never$')"+%s)  
        if [[ "$l_change" -gt "$(date +%s)" ]]; then  
            echo "User: \"$l_user\" last password change was \"$(chage --list  
$l_user | grep '^Last password change' | cut -d: -f2)\""  
            fi  
    done <<(awk -F: '$2~/^\$/+${print $1}' /etc/shadow)  
}
```

#### **Remediation:**

Investigate any users with a password change date in the future and correct them. Locking the account, expiring the password, or resetting the password manually may be appropriate.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.</p>	●	●	●
v7	<p><b>4.4 Use Unique Passwords</b> 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>		●	●

## 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		

## **5.4.2 Configure root and system accounts and environment**

### *5.4.2.1 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:**

Run the following command to change the `root` account UID to 0:

```
# usermod -u 0 root
```

Modify any users other than `root` with UID 0 and assign them a new UID.

#### **References:**

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

#### **MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.000	TA0001	M1026

### *5.4.2.2 Ensure root is the only GID 0 account (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `usermod` command can be used to specify which group the `root` account belongs to. This affects permissions of files that are created by the `root` account.

#### **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 to verify the `root` user's primary GID is 0, and no other user's have GID 0 as their primary GID:

```
# awk -F: '$1 !~ /^(sync|shutdown|halt|operator)/ && $4=="0") {print $1":$4}' /etc/passwd  
root:0
```

**Note:** User's: sync, shutdown, halt, and operator are excluded from the check for other user's with GID 0

#### **Remediation:**

Run the following command to set the `root` user's GID to 0:

```
# usermod -g 0 root
```

Run the following command to set the `root` group's GID to 0:

```
# groupmod -g 0 root
```

Remove any users other than the `root` user with GID 0 or assign them a new GID if appropriate.

#### **References:**

1. 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><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1548, T1548.000	TA0005	M1026

### *5.4.2.3 Ensure group root is the only GID 0 group (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `groupmod` command can be used to specify which group the `root` group belongs to. This affects permissions of files that are group owned by the `root` group.

#### **Rationale:**

Using GID 0 for the `root` group helps prevent `root` group owned files from accidentally becoming accessible to non-privileged users.

#### **Audit:**

Run the following command to verify no group other than `root` is assigned GID 0:

```
# awk -F: '$3=="0"{print $1":"$3}' /etc/group
root:0
```

#### **Remediation:**

Run the following command to set the `root` group's GID to 0:

```
# groupmod -g 0 root
```

Remove any groups other than the `root` group with GID 0 or assign them a new GID if appropriate.

#### **References:**

1. 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><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1548, T1548.000	TA0005	M1026

#### *5.4.2.4 Ensure root password is set (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

There are a number of methods to access the root account directly. Without a password set any user would be able to gain access and thus control over the entire system.

##### **Rationale:**

Access to `root` should be secured at all times.

##### **Impact:**

If there are any automated processes that relies on access to the root account without authentication, they will fail after remediation.

##### **Audit:**

Run the following command to verify the root user's password is set:

```
# passwd -S root | awk '$2 ~ /P/ {print "User: \"\$1\" Password is set"}'  
User: "root" Password is set
```

##### **Remediation:**

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

```
# passwd root
```

##### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1078	TA0005	M1026

### *5.4.2.5 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 to verify root's path does not include:

- Locations that are not directories
- An empty directory (::)
- A trailing (:
- Current working directory (.)
- Non root owned directories
- Directories that less restrictive than mode 0755

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

{
    l_output2=""
    l_pmask="0022"
    l_maxperm=$( printf '%o' $(( 0777 & ~$l_pmask )) )
    l_root_path=$(sudo -Hiu root env | grep '^PATH' | cut -d= -f2)
    unset a_path_loc && IFS=: read -ra a_path_loc <<< "$l_root_path"
    grep -q "::" <<< "$l_root_path" && l_output2="$l_output2\n - root's path
contains a empty directory (::)"
    grep -Pq ":\h*\$" <<< "$l_root_path" && l_output2="$l_output2\n - root's
path contains a trailing (:)"
    grep -Pq '(\h+|:)\.(.:|\h*\$)' <<< "$l_root_path" && l_output2="$l_output2\n
- root's path contains current working directory (.)"
    while read -r l_path; do
        if [ -d "$l_path" ]; then
            while read -r l_fmode l_fown; do
                [ "$l_fown" != "root" ] && l_output2="$l_output2\n - Directory:
\"$l_path\" is owned by: \"$l_fown\" should be owned by \"root\""
                [ $(( $l_fmode & $l_pmask )) -gt 0 ] && l_output2="$l_output2\n
- Directory: \"$l_path\" is mode: \"$l_fmode\" and should be mode:
\"$l_maxperm\" or more restrictive"
                done <<< "$(stat -Lc '%#a %U' \"$l_path\")"
            else
                l_output2="$l_output2\n - \"$l_path\" is not a directory"
            fi
        done <<< "$(printf "%s\n" "${a_path_loc[@]}")"
        if [ -z "$l_output2" ]; then
            echo -e "\n- Audit Result:\n *** PASS ***\n - Root's path is correctly
configured\n"
        else
            echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit
failure * :\n$l_output2\n"
        fi
    }
}
```

## **Remediation:**

### Correct or justify any:

- Locations that are not directories
  - Empty directories (:) (.)
  - Trailing (.)
  - Current working directory (.)
  - Non root owned directories
  - Directories that less restrictive than mode 0755

## References:

- ## 1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0006	M1022

### *5.4.2.6 Ensure root user umask is configured (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-----`.

#### **root user Shell Configuration Files:**

- `/root/.bash_profile` - Is executed to configure the root users' shell before the initial command prompt. **Is only read by login shells.**
- `/root/.bashrc` - Is executed for interactive shells. **only read by a shell that's both interactive and non-login**

`umask` is set by order of precedence. If `umask` is set in multiple locations, this order of precedence will determine the system's default `umask`.

#### **Order of precedence:**

1. `/root/.bash_profile`
2. `/root/.bashrc`
3. The system default `umask`

## Rationale:

Setting a secure value for `umask` ensures that users make a conscious choice about their file permissions. A permissive `umask` value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

## Audit:

Run the following to verify the root user `umask` is set to enforce a newly created directories' permissions to be `750` (`drwxr-x---`), and a newly created file's permissions be `640` (`rw-r-----`), or more restrictive:

```
grep -Psi -- '^h*umask\h+(([0-7][0-7][01][0-7]\b|[0-7][0-7][0-7][0-6]\b)|([0-7][01][0-7]\b|[0-7][0-7][0-6]\b)|(u=[rwx]{1,3},)?((g=[rx]?)?w[rx]?[rx]?\b)(,o=[rwx]{1,3})?)|((g=[rwx]{1,3},)?o=[rwx]{1,3}\b))' /root/.bash_profile /root/.bashrc
```

Nothing should be returned

## Remediation:

Edit `/root/.bash_profile` and `/root/.bashrc` and remove, comment out, or update any line with `umask` to be `0027` or more restrictive.

## Default Value:

System default `umask`

## References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1083	TA0007	

### *5.4.2.7 Ensure system accounts do not have a valid login shell (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. Furthermore, a user may add special accounts that 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 command to verify system accounts, except for `root`, `halt`, `sync`, `shutdown` or `nfsnobody`, do not have a valid login shell:

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

{
    l_valid_shells="^$(awk -F'\| '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^//{s/,/\n/g;p}' | paste -s -d '|')$"
    awk -v pat="$l_valid_shells" -F:
'($1!~^(root|halt|sync|shutdown|nfsnobody)$) && ($3<"$(awk
'/^\s*UID_MIN/{print $2}' /etc/login.defs)" || $3 == 65534) && $(NF) ~ pat
{print "Service account: \"\$1\" has a valid shell: \"\$7\"'} /etc/passwd
'}
```

Nothing should be returned

## Remediation:

Run the following command to set the shell for any service accounts returned by the audit to `nologin`:

```
# usermod -s $(command -v nologin) <user>
```

*Example script:*

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

{
    l_valid_shells="^($(`awk -F\` '$NF != "nologin" {print}' /etc/shells | sed -rn '/^//{s/,/\`/g;p}' | paste -s -d '\`' - `))$"
    awk -v pat="$l_valid_shells" -F:
    '($1!~/^(root|halt|sync|shutdown|nfsnobody)$/ && ($3<'"$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)"' || $3 == 65534) && $(NF) ~ pat)
    {system ("usermod -s '"$(command -v nologin)"' '$1')}' /etc/passwd
}
```

## References:

1. NIST SP 800-53 Rev. 5: AC-2(5), AC-3, AC-11, MP-2

## Additional Information:

The `root`, `sync`, `shutdown`, and `halt` users are exempted from requiring a non-login shell.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1078, T1078.001, T1078.003	TA0005	M1026

### *5.4.2.8 Ensure accounts without a valid login shell are locked (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. Furthermore, a user may add special accounts that 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 script to verify all non-root accounts without a valid login shell are locked.

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

{
    l_valid_shells="^$(awk -F\/ '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^//{s/,/\n/g;p}' | paste -s -d '|' - )$"
    while IFS= read -r l_user; do
        passwd -S "$l_user" | awk '$2 !~ /L/ {print "Account: \"\$1\" does
not have a valid login shell and is not locked"}'
        done < <(awk -v pat="$l_valid_shells" -F: '($1 != "root" && $(NF) !~ pat)
{print \$1}' /etc/passwd)
}
```

Nothing should be returned

## Remediation:

Run the following command to lock any non-root accounts without a valid login shell returned by the audit:

```
# usermod -L <user>
```

*Example script::*

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

{
    l_valid_shells="^($(awk -F\/ '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^//{s/,/\n/g;p}' | paste -s -d '|')$"
    while IFS= read -r l_user; do
        passwd -S "$l_user" | awk '$2 !~ /L/ {system ("usermod -L " $1)}"
        done < <(awk -v pat="$l_valid_shells" -F: '($1 != "root" && $(NF) !~ pat
{print $1}') /etc/passwd)
    }
```

## References:

1. NIST SP 800-53 Rev. 5: AC-2(5), AC-3, AC-11, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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
T1078, T1078.001, T1078.003	TA0005	M1026

### **5.4.3 Configure user default environment**

### *5.4.3.1 Ensure nologin is not listed in /etc/shells (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

/etc/shells is a text file which contains the full pathnames of valid login shells. This file is consulted by chsh and available to be queried by other programs.

Be aware that there are programs which consult this file to find out if a user is a normal user; for example, FTP daemons traditionally disallow access to users with shells not included in this file.

#### **Rationale:**

A user can use chsh to change their configured shell.

If a user has a shell configured that isn't in /etc/shells, then the system assumes that they're somehow restricted. In the case of chsh it means that the user cannot change that value.

Other programs might query that list and apply similar restrictions.

By putting nologin in /etc/shells, any user that has nologin as its shell is considered a full, unrestricted user. This is not the expected behavior for nologin.

#### **Audit:**

Run the following command to verify that nologin is not listed in the /etc/shells file:

```
# grep '/nologin\b' /etc/shells
```

Nothing should be returned

#### **Remediation:**

Edit /etc/shells and remove any lines that include nologin

#### **References:**

1. shells(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

### **5.4.3.2 Ensure default user shell timeout is configured (Automated)**

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

`TMOUT` is an environmental setting that determines the timeout of a shell in seconds.

- `TMOUT=n` - Sets the shell timeout to *n* seconds. A setting of `TMOUT=0` disables timeout.
- `readonly TMOUT` - Sets the `TMOUT` environmental variable as readonly, preventing unwanted modification during run-time.
- `export TMOUT` - exports the `TMOUT` variable

#### **System Wide Shell Configuration Files:**

- `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `.bash_profile`, however this file is used to set an initial PATH or PS1 for all shell users of the system. **is only executed for interactive login shells, or shells executed with the --login parameter.**
- `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh`. It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
- `/etc/bashrc` - System wide version of `.bashrc`. In Fedora derived distributions, `/etc/bashrc` also invokes `/etc/profile.d/*.sh` if *non-login* shell, but redirects output to `/dev/null` if *non-interactive*. **Is only executed for interactive shells or if BASH\_ENV is set to /etc/bashrc.**

#### **Rationale:**

Setting a timeout value reduces the window of opportunity for unauthorized user access to another user's shell session that has been left unattended. It also ends the inactive session and releases the resources associated with that session.

## Audit:

Run the following script to verify that TMOUT is configured to: include a timeout of no more than 900 seconds, to be readonly, to be exported, and is not being changed to a longer timeout.

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

{
    output1="" output2=""
    [ -f /etc/bashrc ] && BRC="/etc/bashrc"
    for f in "$BRC" /etc/profile /etc/profile.d/*.sh ; do
        grep -Pq '^s*([^\#]+\s+)?TMOUT=(900|[1-8][0-9][0-9]|1[1-9][0-9]|1[1-9])\b' "$f" && grep -Pq
        '^s*([^\#]+\s+)?readonly\s+TMOUT(\s+|\s*;|\s*\$|=(900|[1-8][0-9][0-9]|1[1-9][0-9]|1[1-9]))\b' "$f" && grep -Pq
        '^s*([^\#]+\s+)?export\s+TMOUT(\s+|\s*;|\s*\$|=(900|[1-8][0-9][0-9]|1[1-9][0-9]|1[1-9]))\b' "$f" &&
        output1="$f"
    done
    grep -Pq '^s*([^\#]+\s+)?TMOUT=(9[0-9][1-9]|9[1-9][0-9]|0+[1-9]\d{3,})\b'
    /etc/profile /etc/profile.d/*.sh "$BRC" && output2=$(grep -Ps
    '^s*([^\#]+\s+)?TMOUT=(9[0-9][1-9]|9[1-9][0-9]|0+[1-9]\d{3,})\b'
    /etc/profile /etc/profile.d/*.sh $BRC)
    if [ -n "$output1" ] && [ -z "$output2" ]; then
        echo -e "\nPASSED\nTMOUT is configured in: \"$output1\"\n"
    else
        [ -z "$output1" ] && echo -e "\nFAILED\nTMOUT is not configured\n"
        [ -n "$output2" ] && echo -e "\nFAILED\nTMOUT is incorrectly
configured in: \"$output2\"\n"
    fi
}
```

## Remediation:

Review `/etc/bashrc`, `/etc/profile`, and all files ending in `*.sh` in the `/etc/profile.d/` directory and remove or edit all `TMOUT=_n_` entries to follow local site policy. `TMOUT` should not exceed 900 or be equal to 0.

Configure `TMOUT` in **one** of the following files:

- A file in the `/etc/profile.d/` directory ending in `.sh`
- `/etc/profile`
- `/etc/bashrc`

*TMOUT configuration examples:*

- As multiple lines:

```
TMOUT=900
readonly TMOUT
export TMOUT
```

- As a single line:

```
readonly TMOUT=900 ; export TMOUT
```

## Additional Information:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked. Other methods of setting a timeout exist for other shells not covered here.

Ensure that the timeout conforms to your local policy.

## CIS Controls:

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

**MITRE ATT&CK Mappings:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1078	TA0005	M1026

### *5.4.3.3 Ensure default user umask is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The user file-creation mode mask (`umask`) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (`rwxrwxrwx`), and for any newly created file it is 0666 (`rw-rw-rw-`). The `umask` modifies the default Linux permissions by restricting (masking) these permissions. The `umask` is not simply subtracted, but is processed bitwise. Bits set in the `umask` are cleared in the resulting file mode.

`umask` can be set with either Octal or Symbolic values:

- Octal (Numeric) Value - Represented by either three or four digits. ie `umask 0027` or `umask 027`. If a four digit umask is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- Symbolic Value - Represented by a comma separated list for User `u`, group `g`, and world/other `o`. The permissions listed are not masked by `umask`. ie a `umask set by umask u=rwx,g=rx,o=` is the Symbolic equivalent of the Octal umask 027. This `umask` would set a newly created directory with file mode `drwxr-x---` and a newly created file with file mode `rw-r-----`.

The default `umask` can be set to use the `pam_umask` module or in a System Wide Shell Configuration File. The user creating the directories or files has the discretion of changing the permissions via the `chmod` command, or choosing a different default `umask` by adding the `umask` command into a User Shell Configuration File, (`.bash_profile` or `.bashrc`), in their home directory.

## Setting the default umask:

- pam\_umask module:
  - will set the umask according to the system default in `/etc/login.defs` and user settings, solving the problem of different `umask` settings with different shells, display managers, remote sessions etc.
  - `umask=<mask>` value in the `/etc/login.defs` file is interpreted as Octal
  - Setting `USERGROUPS_ENAB` to yes in `/etc/login.defs` (default):
    - will enable setting of the `umask` group bits to be the same as owner bits. (examples: 022 -> 002, 077 -> 007) for non-root users, if the `uid` is the same as `gid`, and `username` is the same as the `<primary group name>`
    - `userdel` will remove the user's group if it contains no more members, and `useradd` will create by default a group with the name of the user
- System Wide Shell Configuration File:
  - `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `.bash_profile`, however this file is used to set an initial PATH or PS1 for all shell users of the system. **is only executed for interactive login shells, or shells executed with the --login parameter.**
  - `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh`. It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
  - `/etc/bashrc` - System wide version of `.bashrc`. In Fedora derived distributions, `etc/bashrc` also invokes `/etc/profile.d/*.sh` if *non-login* shell, but redirects output to `/dev/null` if *non-interactive*. **Is only executed for interactive shells or if BASH\_ENV is set to /etc/bashrc.**

## User Shell Configuration Files:

- `~/.bash_profile` - Is executed to configure your shell before the initial command prompt. **Is only read by login shells.**
- `~/.bashrc` - Is executed for interactive shells. **only read by a shell that's both interactive and non-login**

`umask` is set by order of precedence. If `umask` is set in multiple locations, this order of precedence will determine the system's default `umask`.

## **Order of precedence:**

1. A file in `/etc/profile.d/` ending in `.sh` - This will override any other system-wide `umask` setting
2. In the file `/etc/profile`
3. On the `pam_umask.so` module in `/etc/pam.d/postlogin`
4. In the file `/etc/login.defs`
5. In the file `/etc/default/login`

## **Rationale:**

Setting a secure default value for `umask` ensures that users make a conscious choice about their file permissions. A permissive `umask` value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

## Audit:

Run the following to verify the default user `umask` is set to enforce a newly created directories' permissions to be `750` (`drwxr-x---`), and a newly created file's permissions be `640` (`rw-r-----`), or more restrictive:

## Remediation:

Run the following script and perform the instructions in the output:

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

{
    l_output="" l_output2="" l_out=""
    file_umask_chk()
    {
        if grep -Psiq -- '^h*umask\h+(0?[0-7][2-
7]7|u(=[rwx]{0,3}),g=([rx]{0,2}),o=(\h*#.*)?${' "$l_file"; then
            l_out="$l_out\n - umask is set correctly in \"$l_file\""
        elif grep -Psiq -- '^h*umask\h+(([0-7][0-7][01][0-7]\b|[0-7][0-7][0-
7][0-6]\b)|([0-7][01][0-7]\b|[0-7][0-7][0-
6]\b)|(u=[rwx]{1,3},)?(((g=[rx]?[rx]?w[rx]?[rx]?b),(o=[rwx]{1,3}))|((g=[rwx
]{1,3}),?o=[rwx]{1,3}\b)))' "$l_file"; then
            l_output2="$l_output2\n - \"$l_file\""
        fi
    }
    while IFS= read -r -d $'\0' l_file; do
        file_umask_chk
        done <<(find /etc/profile.d -type f -name '*.sh' -print0)
        [ -n "$l_out" ] && l_output="$l_out"
        l_file="/etc/profile" && file_umask_chk
        l_file="/etc/bashrc" && file_umask_chk
        l_file="/etc/bash.bashrc" && file_umask_chk
        l_file="/etc/pam.d/postlogin"
        if grep -Psiq
'^h*session\h+[^#\n\r]+\h+pam_umask\.so\h+([^\#\n\r]+\h+)?umask=(([0-7][0-
7][01][0-7]\b|[0-7][0-7][0-7][0-6]\b)|([0-7][01][0-7]\b))' "$l_file"; then
            l_output2="$l_output2\n - \"$l_file\""
        fi
        l_file="/etc/login.defs" && file_umask_chk
        l_file="/etc/default/login" && file_umask_chk
        if [ -z "$l_output2" ]; then
            echo -e "\n - No files contain a UMASK that is not restrictive enough\n"
        No UMASK updates required to existing files"
        else
            echo -e "\n - UMASK is not restrictive enough in the following
file(s):$l_output2\n\n- Remediation Procedure:\n - Update these files and
comment out the UMASK line\n or update umask to be \"0027\" or more
restrictive"
        fi
        if [ -n "$l_output" ]; then
            echo -e "$l_output"
        else
            echo -e "\n - Configure UMASK in a file in the \"/etc/profile.d/\""
directory ending in \".\sh\"\n\n Example Command (Hash to represent being
run at a root prompt):\n\n# printf '%s\\n' \"umask 027\" >
/etc/profile.d/50-systemwide_umask.sh\n"
        fi
    }
}
```

**Notes:**

- 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
- If the `pam_umask.so` module is going to be used to set `umask`, ensure that it's not being overridden by another setting. Refer to the PAM\_UMASK(8) man page for more information

**Default Value:**

UMASK 022

**References:**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

**Additional Information:**

- Other methods of setting a default user umask exist
- If other methods are in use in your environment they should be audited
- The default user umask can be overridden with a user specific umask
- The user creating the directories or files has the discretion of changing the permissions:
  - Using the `chmod` command
  - Setting a different default umask by adding the `umask` command into a User Shell Configuration File, (`.bashrc`), in their home directory
  - Manually changing the umask for the duration of a login session by running the `umask` command

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1083	TA0007	

## 6 Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included in most distributions.

It is recommended that `rsyslog` be used for logging (with `logwatch` providing summarization) and `auditd` be used for auditing (with `aureport` providing summarization) to automatically monitor logs for intrusion attempts and other suspicious system behavior.

In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server via an encrypted connection. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices. Reference <<http://chrony.tuxfamily.org/>> manual page for more information on configuring chrony.

It is important that all logs described in this section be monitored on a regular basis and correlated to determine trends. A seemingly innocuous entry in one log could be more significant when compared to an entry in another log.

**Note on log file permissions:** There really isn't a "one size fits all" solution to the permissions on log files. Many sites utilize group permissions so that administrators who are in a defined security group, such as "wheel" do not have to elevate privileges to root in order to read log files. Also, if a third party log aggregation tool is used, it may need to have group permissions to read the log files, which is preferable to having it run setuid to root. Therefore, there are two remediation and audit steps for log file permissions. One is for systems that do not have a secured group method implemented that only permits root to read the log files (`root:root 600`). The other is for sites that do have such a setup and are designated as `root:securegrp 640` where `securegrp` is the defined security group (in some cases `wheel`).

## **6.1 Configure 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.

### *6.1.1 Ensure AIDE is installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Run the following command to verify aide is installed:

```
# dpkg-query -s aide &>/dev/null && echo "aide is installed"  
aide is installed
```

Run the following command to verify aide-common is installed:

```
# dpkg-query -s aide-common &>/dev/null && echo "aide-common is installed"  
aide-common is 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
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-2

### **Additional Information:**

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

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.14 Log Sensitive Data Access</b> Log sensitive data access, including modification and disposal.			●
v7	<b>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</b> 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
T1036, T1036.002, T1036.003, T1036.004, T1036.005, T1565, T1565.001		

## *6.1.2 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 -Prs '^([^\n\r]+\h+)?(/usr/s?bin/|^h*)aide(\.wrapper)?\h+(--(check|update)|([^\n\r]+\h+)?\$AIDEARGS)\b' /etc/cron.* /etc/crontab  
/var/spool/cron/
```

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

- OR -

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

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

## **Remediation:**

If cron will be used to schedule and run aide check:

Run the following command:

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

Add the following line to the crontab:

```
0 5 * * * /usr/bin/aide.wrapper --config /etc/aide/aide.conf --update
```

- 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 --update

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

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

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

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

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

Run the following commands:

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

# systemctl daemon-reload

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

## **References:**

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

## **Additional Information:**

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

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

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

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</b> 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
T1036, T1036.002, T1036.003, T1036.004, T1036.005, T1565, T1565.001	TA0040	M1022

### *6.1.3 Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - 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 script to verify:

- AIDE is configured to use cryptographic mechanisms to protect the integrity of audit tools:
- The following audit tool files include the options "p, i, n, u, g, s, b, acl, xattrs and sha512"
  - /sbin/auditctl
  - /sbin/auditd
  - /sbin/ausearch
  - /sbin/aureport
  - /sbin/autrace
  - /sbin/augenrules

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    f_parameter_chk()
    {
        l_out="" l_out2=""
        for l_string in "${!A_out[@]}"; do
            l_file_parameter=$(grep -Po -- "\^\\h*\$l_parameter_name\\b.*\$" <<< "$l_string")
            if [ -n "$l_file_parameter" ]; then
                l_file=$(printf '%s' "${A_out[$l_file_parameter]}")
                l_out="$l_out\n - Exists as: \"$l_file_parameter\"\n - in the configuration file:
\"$l_file\""
                for l_var in "${a_items[@]}"; do
                    if ! grep -Pq -- "\b\$l_var\b" <<< "$l_file_parameter"; then
                        l_out2="$l_out2\n - Option: \"$l_var\" is missing from: \"$l_file_parameter\""
                    fi
                done
                fi
            done
            [ -n "$l_out" ] && l_output="$l_output\n - Parameter: \"$l_parameter_name\":$l_out"
            [ -z "$l_out2" ] && l_output="$l_output\n - and includes \"$(printf '%s+
${a_items[@]}')\""
            [ -n "$l_out2" ] && l_output2="$l_output2\n - Parameter: \"$l_parameter_name\":$l_out2"
            [[ -z "$l_out" && -z "$l_out2" ]] && l_output2="$l_output2\n - Parameter:
\"$l_parameter_name\" is not configured"
        }
        f_check_config()
        {
            a_items=(p i n u g s b acl xattrs sha512)
            a_parlist=(/sbin/auditctl "/sbin/auditd" "/sbin/ausearch" "/sbin/aureport"
"/sbin/autrace" "/sbin/augenrules")
            unset A_out; declare -A A_out
            while IFS= read -r l_out; do
                if [ -n "$l_out" ]; then
                    if [[ $l_out =~ ^\s*# ]]; then
                        l_file="${l_out//#/ }"
                    else
                        l_parameter="$l_out"
                        A_out+=(["$l_parameter"]="$l_file")
                    fi
                fi
            done < <(/usr/bin/systemd-analyze cat-config "$l_config_file" | grep -Pio
'^\\h*([^\#\\n\\r]+\\h*/[^#\\n\\r\\h]+\!.conf\\b)')
            for l_parameter_name in "${a_parlist[@]}"; do
                if [ -f "$l_parameter_name" ]; then
                    f_parameter_chk
                else
                    l_output="$l_output\n - ** Warning **\n   Audit tool file: \"$l_parameter_name\" does
not exist\n   Please verify auditd is installed"
                    fi
                done
            }
            if [ -f "/etc/aide/aide.conf" ]; then
                l_config_file="/etc/aide/aide.conf" && f_check_config
            elif [ -f "/etc/aide.conf" ]; then
                l_config_file="/etc/aide.conf" && f_check_config
            else
                l_output2="$l_output2\n - AIDE configuration file not found.\n   Please verify AIDE is
installed on the system"
            fi
            unset a_items; unset a_parlist; unset A_out
            if [ -z "$l_output2" ]; then
                echo -e "\n- Audit Result:\n   ** PASS **\n   * Correctly configured * :$l_output"
            else
                echo -e "\n- Audit Result:\n   ** FAIL **\n   * Reasons for audit failure * :$l_output2\n"
                [ -n "$l_output" ] && echo -e "\n   * Correctly configured * :\n$l_output\n"
            fi
        }
}

```

**Note:** The script is written to read the "winning" configuration setting, to include any configuration settings in files included as part of the `@@x_include` setting.

### Remediation:

Edit `/etc/aide/aide.conf` and add or update the following selection lines:

```
# 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
```

**Note: - IF -** /etc/aide/aide.conf includes a `@@x_include` statement:

*Example:*

```
@@x_include /etc/aide/aide.conf.d ^[a-zA-Z0-9_-]+$
```

- `@@x_include FILE`
- `@@x_include DIRECTORY REGEX`
  - `@@x_include` is identical to `@@include`, except that if a config file is executable it is run and the output is used as config.
  - If the executable file exits with status greater than zero or writes to stderr aide stops with an error.
  - For security reasons DIRECTORY and each executable config file must be owned by the current user and must not be group or world-writable.

### References:

1. AIDE.CONF(5)

### MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

## 6.2 System 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 `journald`.

- If your organization makes use of another logging system such as `rsyslog` or an enterprise wide logging system completely outside of `journald`, then the following recommendations do not directly apply. However, the principals of the recommendations should be followed regardless of what solution is implemented. If the enterprise solution incorporates `journald`, careful consideration should be given to the following recommendations to determine exactly what applies.

### What is not covered

- Enterprise logging systems not utilizing `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. `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.

### **6.2.1 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.service`

### 6.2.1.1 Configure systemd-journald service

`systemd-journald` is a system service that collects and stores logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources:

- Kernel log messages, via `kmsg`
- Simple system log messages, via the `libc syslog` call
- Structured system log messages via the native Journal API
- Standard output and standard error of service units
- Audit records, originating from the kernel audit subsystem

The daemon will implicitly collect numerous metadata fields for each log message in a secure and unfakeable way. See `systemd.journal-fields` man page for more information about the collected metadata.

The journal service stores log data either persistently below `/var/log/journal` or in a volatile way below `/run/log/journal/`. By default, log data is stored persistently if `/var/log/journal/` exists during boot, with an implicit fallback to volatile storage. Use `Storage=` in `journald.conf` to configure where log data is placed, independently of the existence of `/var/log/journal/`.

On systems where `/var/log/journal/` does not exist but where persistent logging is desired, and the default `journald.conf` is used, it is sufficient to create the directory and ensure it has the correct access modes and ownership.

### *6.2.1.1 Ensure journald service is enabled and active (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
static
```

**Note:** 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. Run the following command to verify `systemd-journald` is active:

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

#### **Remediation:**

Run the following commands to unmask and start `systemd-journald.service`

```
# systemctl unmask systemd-journald.service
# systemctl start systemd-journald.service
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-7 AU-12

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> 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	M1029

### *6.2.1.1.2 Ensure journald log file access is 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 determine 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 no override file exists, inspect the default `/usr/lib/tmpfiles.d/systemd.conf` against the site specific requirements.

Ensure that file permissions are mode `0640` or more restrictive.

#### **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.

#### **References:**

1. NIST SP 800-53 Rev. 5: AC-3, AU-2, AU-12, MP-2, SI-5

#### **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><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	M1022

### *6.2.1.1.3 Ensure journald log file rotation is configured (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 files in the `/etc/systemd/journald.conf.d/` directory ending in `.conf`. Verify logs are rotated according to site policy. The specific parameters for log rotation are:

```
SystemMaxUse=
SystemKeepFree=
RuntimeMaxUse=
RuntimeKeepFree=
MaxFileSec=
```

#### **Remediation:**

Edit `/etc/systemd/journald.conf` or a file ending in `.conf` in the `/etc/systemd/journald.conf.d/` directory. Set the following parameters in the [Journal] section to ensure logs are rotated according to site policy. The settings should be carefully understood as there are specific edge cases and prioritization of parameters.

The specific parameters for log rotation are:

```
SystemMaxUse=
SystemKeepFree=
RuntimeMaxUse=
RuntimeKeepFree=
MaxFileSec=
```

**Note:** If these settings appear in a canonically later file, or later in the same file, the setting will be overwritten

## References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-7, AU-12

## 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	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> 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	TA0040	M1022

#### *6.2.1.1.4 Ensure journald ForwardToSyslog is disabled (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Data from `journald` should be kept in the confines of the service and not forwarded to other services.

##### **Rationale:**

Logs of the system should be handled by `journald` and not forwarded to other logging mechanisms.

## Audit:

Run the following script to verify `ForwardToSyslog` in not set to yes:

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

{
    l_output="" l_output2=""
    a_parlist=("ForwardToSyslog=yes")
    l_systemd_config_file="/etc/systemd/journald.conf" # Main systemd configuration file
    config_file_parameter_chk()
    {
        unset A_out; declare -A A_out # Check config file(s) setting
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out##*/# }"
                else
                    l_systemd_parameter=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    grep -Piq -- "^\h*$l_systemd_parameter\b" <<< "$l_systemd_parameter" &&
                    A_out+=(["$l_systemd_parameter"]="$l_file")
                fi
            fi
        done < <(/usr/bin/systemd-analyze cat-config "$l_systemd_config_file" | grep -Pio
        '^\h*([^\#\n\r]+|\#\h*/[^\#\n\r\h]+\.\conf\b)')
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="=" read -r l_systemd_file_parameter_name l_systemd_file_parameter_value; do
                l_systemd_file_parameter_name="${l_systemd_file_parameter_name// /}"
                l_systemd_file_parameter_value="${l_systemd_file_parameter_value// /}"
                if ! grep -Piq "^\h*$l_systemd_file_parameter_value\b" <<<
                "$l_systemd_file_parameter_value"; then
                    l_output="$l_output\n - \\"$l_systemd_file_parameter_name\\\" is correctly set to
                    \\\"$l_systemd_file_parameter_value\\\" in \\\"$printf '%s' \"${A_out[@]}\"\\"\\n"
                else
                    l_output2="$l_output2\n - \\"$l_systemd_file_parameter_name\\\" is incorrectly set to
                    \\\"$l_systemd_file_parameter_value\\\" in \\\"$printf '%s' \"${A_out[@]}\"\\"\\n"
                fi
            done < <(grep -Pio -- "^\h*$l_systemd_file_parameter_name\b=\h*\H+" "${A_out[@]}")
        else
            l_output="$l_output\n - \\"$l_systemd_file_parameter_name\\\" is not set in an included file\\n
** Note: \\\"$l_systemd_file_parameter_name\\\" May be set in a file that's ignored by load procedure
**\\n"
        fi
    }
    while IFS="=" read -r l_systemd_parameter_name l_systemd_parameter_value; do # Assess and
    check parameters
        l_systemd_parameter_name="${l_systemd_parameter_name// /}"
        l_systemd_parameter_value="${l_systemd_parameter_value// /}"
        config_file_parameter_chk
    done < <(printf '%s\\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        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:**

Set the following parameter in the [Journal] section in /etc/systemd/journald.conf or a file in /etc/systemd/journald.conf.d/ ending in .conf:

```
ForwardToSyslog=no
```

### *Example:*

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

{
    [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir
/etc/systemd/journald.conf.d/
    if grep -Psq -- '^h*\[Journal\]' /etc/systemd/journald.conf.d/60-
journald.conf; then
        printf '%s\n' "ForwardToSyslog=no" >> /etc/systemd/journald.conf.d/60-
journald.conf
    else
        printf '%s\n' "[Journal]" "ForwardToSyslog=no" >>
/etc/systemd/journald.conf.d/60-journald.conf
    fi
}
```

**Note:** If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run the following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

### **Default Value:**

ForwardToSyslog=no

### **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-6, AU-7, AU-12

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

### *6.2.1.1.5 Ensure journald Storage is configured (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:

Run the following script to verify Storage is set to persistent:

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

{
    l_output="" l_output2=""
    a_parlist=("Storage=persistent")
    l_systemd_config_file="/etc/systemd/journald.conf" # Main systemd configuration file
    config_file_parameter_chk()
    {
        unset A_out; declare -A A_out # Check config file(s) setting
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//#/ }"
                else
                    l_systemd_parameter=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    grep -Piq -- "^\h*$l_systemd_parameter\b" <<< "$l_systemd_parameter" &&
                    A_out+=(["$l_systemd_parameter"]="$l_file")
                fi
            fi
        done < <(/usr/bin/systemd-analyze cat-config "$l_systemd_config_file" | grep -Pio
        '^h*([^\n\r]+|#[^\n\r]+\.[^\n\r\h]+\.\conf\b)')
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="=" read -r l_systemd_file_parameter_name l_systemd_file_parameter_value; do
                l_systemd_file_parameter_name="${l_systemd_file_parameter_name// /}"
                l_systemd_file_parameter_value="${l_systemd_file_parameter_value// /}"
                if grep -Piq "^\h*$l_systemd_file_parameter_value\b" <<
                "$l_systemd_file_parameter_value"; then
                    l_output="$l_output\n - \"$l_systemd_file_parameter_name\" is correctly set to
                    \"$l_systemd_file_parameter_value\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_systemd_file_parameter_name\" is incorrectly set to
                    \"$l_systemd_file_parameter_value\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value
                    matching: \"$l_systemd_file_parameter_value\"\n"
                fi
            done < <(grep -Pio -- "^\h*$l_systemd_file_parameter_name\b*=h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_systemd_file_parameter_name\" is not set in an included file\n"
        ** Note: \"$l_systemd_file_parameter_name\" May be set in a file that's ignored by load procedure
        **\n"
        fi
    }
    while IFS="=" read -r l_systemd_parameter_name l_systemd_parameter_value; do # Assess and
    check parameters
        l_systemd_parameter_name="${l_systemd_parameter_name// /}"
        l_systemd_parameter_value="${l_systemd_parameter_value// /}"
        config_file_parameter_chk
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}
```

## **Remediation:**

Set the following parameter in the [Journal] section in /etc/systemd/journald.conf or a file in /etc/systemd/journald.conf.d/ ending in .conf:

```
Storage=persistent
```

*Example:*

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

{
    [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir
/etc/systemd/journald.conf.d/
    if grep -Psq -- '^h*[Journal\]' /etc/systemd/journald.conf.d/60-
journald.conf; then
        printf '%s\n' "Storage=persistent" >> /etc/systemd/journald.conf.d/60-
journald.conf
    else
        printf '%s\n' "[Journal]" "Storage=persistent" >>
/etc/systemd/journald.conf.d/60-journald.conf
    fi
}
```

**Note:** If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run the following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1070, T1070.002, T1562, T1562.006	TA0005	M1022

### *6.2.1.1.6 Ensure journald Compress is configured (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:

Run the following script to verify Compress is set to yes:

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

{
    l_output="" l_output2=""
    a_parlist=("Compress=yes")
    l_systemd_config_file="/etc/systemd/journald.conf" # Main systemd configuration file
    config_file_parameter_chk()
    {
        unset A_out; declare -A A_out # Check config file(s) setting
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out##*/# }"
                else
                    l_systemd_parameter=$(awk -F= '{print $1}' <<< "$l_out" | xargs)
                    grep -Piq -- "^\h*$l_systemd_parameter\b" <<< "$l_systemd_parameter" &&
                    A_out+=(["$l_systemd_parameter"]="$l_file")
                fi
            fi
        done < <(/usr/bin/systemd-analyze cat-config "$l_systemd_config_file" | grep -Pio
        '^h*([^\n\r]+|#[^\n\r]+\.[^\n\r\h]+\.\conf\b)')
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="=" read -r l_systemd_file_parameter_name l_systemd_file_parameter_value; do
                l_systemd_file_parameter_name="${l_systemd_file_parameter_name// /}"
                l_systemd_file_parameter_value="${l_systemd_file_parameter_value// /}"
                if grep -Piq "^\h*$l_systemd_file_parameter_value\b" <<<
                "$l_systemd_file_parameter_value"; then
                    l_output="$l_output\n - \"$l_systemd_file_parameter_value\" is correctly set to
                    \"$l_systemd_file_parameter_value\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_systemd_file_parameter_value\" is incorrectly set to
                    \"$l_systemd_file_parameter_value\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value
                    matching: \"$l_systemd_file_parameter_value\"\n"
                fi
            done < <(grep -Pio -- "^\h*$l_systemd_file_parameter_name\b*=h*\H+" "${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_systemd_file_parameter_value\" is not set in an included file\n"
        ** Note: \"$l_systemd_file_parameter_name\" May be set in a file that's ignored by load procedure
        **\n"
        fi
    }
    while IFS="=" read -r l_systemd_parameter_name l_systemd_parameter_value; do # Assess and
    check parameters
        l_systemd_parameter_name="${l_systemd_parameter_name// /}"
        l_systemd_parameter_value="${l_systemd_parameter_value// /}"
        config_file_parameter_chk
    done < <(printf '%s\n' "${a_parlist[@]}")
    if [ -z "$l_output2" ]; then # Provide output from checks
        echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:$l_output\n"
    fi
}
```

## **Remediation:**

Set the following parameter in the [Journal] section in /etc/systemd/journald.conf or a file in /etc/systemd/journald.conf.d/ ending in .conf:

```
Compress=yes
```

*Example:*

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

{
    [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir
/etc/systemd/journald.conf.d/
    if grep -Psq -- '^h*[Journal\]' /etc/systemd/journald.conf.d/60-
journald.conf; then
        printf '%s\n' "Compress=yes" >> /etc/systemd/journald.conf.d/60-
journald.conf
    else
        printf '%s\n' "[Journal]" "Compress=yes" >>
/etc/systemd/journald.conf.d/60-journald.conf
    fi
}
```

**Note:** If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run the following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-4

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	<b>8.3 Ensure Adequate Audit Log Storage</b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	<b>6.4 Ensure adequate storage for logs</b> 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, T1562.001	TA0040	M1053

### **6.2.1.2 Configure `systemd-journal-remote`**

The `systemd-journal-remote` package includes `systemd-journal-upload`.

`systemd-journal-upload` will upload journal entries to the URL specified with `--url=`. This program reads journal entries from one or more journal files, similarly to `journalctl`.

`systemd-journal-upload` transfers the raw content of journal file and uses HTTP as a transport protocol.

`systemd-journal-upload.service` is a system service that uses `systemd-journal-upload` to upload journal entries to a server. It uses the configuration in `journal-upload.conf`.

### *6.2.1.2.1 Ensure systemd-journal-remote is installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Journald `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 centralized 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:**

Run the following command to verify `systemd-journal-remote` is installed.

```
# dpkg-query -s systemd-journal-remote &>/dev/null && echo "systemd-journal-  
remote is installed"  
  
systemd-journal-remote is installed
```

#### **Remediation:**

Run the following command to install `systemd-journal-remote`:

```
# apt install systemd-journal-remote
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-7 AU-12

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> 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

### **6.2.1.2.2 Ensure systemd-journal-remote authentication is configured (Manual)**

## **Profile Applicability:**

- Level 1 - Server
  - Level 1 - Workstation

## Description:

Journald `systemd-journal-upload` supports the ability to send log events it gathers to a remote log host.

## 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:

Run the following command to verify `systemd-journal-upload` authentication is configured:

```
# grep -P '^ *URL=|^ *ServerKeyFile=|^ *ServerCertificateFile=|^ *TrustedCertificateFile=' /etc/systemd/journal-upload.conf
```

Verify the output matches per your environments certificate locations and the URL of the log server:

*Example:*

```
[Upload]
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 or a file in `/etc/systemd/journal-upload.conf.d` ending in `.conf` and ensure the following lines are set in the [Upload] section per your environment:

```
[Upload]
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 reload-or-restart systemd-journal-upload.service
```

## References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-12

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> 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

### *6.2.1.2.3 Ensure systemd-journal-upload is enabled and active (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Journald `systemd-journal-upload` supports the ability to send log events it gathers to a remote log host.

#### **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:**

Run the following command to verify `systemd-journal-upload` is enabled.

```
# systemctl is-enabled systemd-journal-upload.service  
enabled
```

Run the following command to verify `systemd-journal-upload` is active:

```
# systemctl is-active systemd-journal-upload.service  
active
```

#### **Remediation:**

Run the following commands to unmask, enable and start `systemd-journal-upload`:

```
# systemctl unmask systemd-journal-upload.service  
# systemctl --now enable systemd-journal-upload.service
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-12

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> 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

## **6.2.1.2.4 Ensure `systemd-journal-remote` service is not in use (Automated)**

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Journald `systemd-journal-remote` 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` and `systemd-journal-remote.service` are not enabled:

```
# systemctl is-enabled systemd-journal-remote.socket systemd-journal-remote.service | grep -P -- '^enabled'
```

Nothing should be returned

Run the following command to verify `systemd-journal-remote.socket` and `systemd-journal-remote.service` are not active:

```
# systemctl is-active systemd-journal-remote.socket systemd-journal-remote.service | grep -P -- '^active'
```

Nothing should be returned

## **Remediation:**

Run the following commands to stop and mask `systemd-journal-remote.socket` and `systemd-journal-remote.service`:

```
# systemctl stop systemd-journal-remote.socket systemd-journal-remote.service  
# systemctl mask systemd-journal-remote.socket systemd-journal-remote.service
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-7 AU-12

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> 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

## **6.2.2 Configure Logfiles**

### *6.2.2.1 Ensure access to all logfiles has been configured (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, others 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

{
    l_op2="" l_output2=""
    l_uidmin=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
    file_test_chk()
    {
        l_op2=""
        if [ $(($l_mode & $perm_mask)) -gt 0 ]; then
            l_op2="$l_op2\n - Mode: \"$l_mode\" should be \"$maxperm\" or more restrictive"
        fi
        if [[ ! "$l_user" =~ $l_auser ]]; then
            l_op2="$l_op2\n - Owned by: \"$l_user\" and should be owned by \"${l_auser//\// or }\""
        fi
        if [[ ! "$l_group" =~ $l_agroup ]]; then
            l_op2="$l_op2\n - Group owned by: \"$l_group\" and should be group owned by \"${l_agroup//\// or }\""
        fi
        [ -n "$l_op2" ] && l_output2="$l_output2\n - File: \"$l_fname\" is:$l_op2"
    }
    unset a_file && a_file=() # clear and initialize array
    # Loop to create array with stat of files that could possibly fail one of the audits
    while IFS= read -r -d ''\0' l_file; do
        [ -e "$l_file" ] && a_file+=("$(stat -Lc '%n%#a%U%u%G%g' \"$l_file")")
    done < <(find -L /var/log -type f \(-perm /0137 -o ! -user root -o ! -group root \) -print0)
    while IFS='^' read -r l_fname l_mode l_user l_uid l_group l_gid; do
        l_bname="${basename \"$l_fname\")"
        case "$l_bname" in
            lastlog | lastlog.* | wtmp | wtmp.* | wtmp-* | btmp | btmp.* | btmp-* | README)
                perm_mask='0113'
                maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
                l_auser="root"
                l_agroup="(root|utmp)"
                file_test_chk
                ;;
            secure | auth.log | syslog | messages)
                perm_mask='0137'
                maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
                l_auser="(root|syslog)"
                l_agroup="(root|adm)"
                file_test_chk
                ;;
            SSSD | sssd)
                perm_mask='0117'
                maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
                l_auser="(root|SSSD)"
                l_agroup="(root|SSSD)"
                file_test_chk
                ;;
            gdm | gdm3)
                perm_mask='0117'
                maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
                l_auser="root"
                l_agroup="(root|gdm|gdm3)"
                file_test_chk
                ;;
            *.journal | *.journal~)
                perm_mask='0137'
                maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
                l_auser="root"
                l_agroup="(root|systemd-journal)"
                file_test_chk
                ;;
        *) 
            perm_mask='0137'
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_auser="(root|syslog)"
            l_agroup="(root|adm)"
            if [ "$l_uid" -lt "$l_uidmin" ] && [ -z "$(awk -v grp=\"$l_group\" -F: '$1==grp {print $4}' /etc/group)" ]; then
                if [[ ! "$l_user" =~ $l_auser ]]; then

```

```

        l_auser="(root|syslog|$l_user)"
    fi
    if [[ ! "$l_group" =~ $l_agroup ]]; then
        l_tst=""
        while l_out3="" read -r l_duid; do
            [ "$l_duid" -ge "$l_uidmin" ] && l_tst=failed
        done <<< "$ awk -F: '$4=='$l_gid' {print $3}' /etc/passwd"
        [ "$l_tst" != "failed" ] && l_agroup="(root|adm|$l_group)"
    fi
    fi
    file_test_chk
    ;;
esac
done <<< $(printf '%s\n' "${a_file[@]}")"
unset a_file # Clear array
# If all files passed, then we pass
if [ -z "$l_output2" ]; then
    echo -e "\n- Audit Results:\n ** Pass **\n- All files in \"/var/log/\" have appropriate
permissions and ownership\n"
else
    # print the reason why we are failing
    echo -e "\n- Audit Results:\n ** Fail **\n$l_output2"
fi
}

```

## **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

{
    l_op2="" l_output2=""
    l_uidmin=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
    file_test_fix()
    {
        l_op2=""
        l_fuser="root"
        l_fgroup="root"
        if [ $(($l_mode & $perm_mask)) -gt 0 ]; then
            l_op2="$l_op2\n - Mode: \"$l_mode\" should be \"$maxperm\" or more restrictive\n - "
            Removing excess permissions
            chmod "$l_rperms" "$l_fname"
        fi
        if [[ ! "$l_user" =~ $l_auser ]]; then
            l_op2="$l_op2\n - Owned by: \"$l_user\" and should be owned by \"${l_auser//|/ or }\\"\n - "
            Changing ownership to: \"$l_fuser\""
            chown "$l_fuser" "$l_fname"
        fi
        if [[ ! "$l_group" =~ $l_agroup ]]; then
            l_op2="$l_op2\n - Group owned by: \"$l_group\" and should be group owned by \"${l_agroup//|/ or }\\"\n - "
            Changing group ownership to: \"$l_fgroup\""
            chgrp "$l_fgroup" "$l_fname"
        fi
        [ -n "$l_op2" ] && l_output2="$l_output2\n - File: \"$l_fname\" is:$l_op2\n"
    }
    unset a_file && a_file=() # clear and initialize array
    # Loop to create array with stat of files that could possibly fail one of the audits
    while IFS= read -r -d $'\0' l_file; do
        [ -e "$l_file" ] && a_file+=("$(stat -Lc '%n^%#a^%u^%G^%g' \"$l_file")")
    done < <(find -L /var/log -type f \(\ -perm /0137 -o ! -user root -o ! -group root \) -print0)
    while IFS='^' read -r l_fname l_mode l_user l_uid l_group l_gid; do
        l_bname="${basename "$l_fname")"
        case "$l_bname" in
            lastlog | lastlog.* | wtmp | wtmp.* | wtmp-* | btmp | btmp.* | btmp-* | README)
                perm_mask='0113'
                maxperm=$((printf '%o' $(( 0777 & ~$perm_mask)) ))
                l_rperms="ug-x,o-wx"
                l_auser="root"
                l_agroup="(root|utmp)"
                file_test_fix
                ;;
            secure | auth.log | syslog | messages)
                perm_mask='0137'
                maxperm=$((printf '%o' $(( 0777 & ~$perm_mask)) ))
                l_rperms="u-x,g-wx,o-rwx"
                l_auser="(root|syslog)"
                l_agroup="(root|adm)"
                file_test_fix
                ;;
            SSSD | sssd)
                perm_mask='0117'
                maxperm=$((printf '%o' $(( 0777 & ~$perm_mask)) ))
                l_rperms="ug-x,o-rwx"
                l_auser="(root|SSSD)"
                l_agroup="(root|SSSD)"
                file_test_fix
                ;;
            gdm | gdm3)
                perm_mask='0117'
                l_rperms="ug-x,o-rwx"
                maxperm=$((printf '%o' $(( 0777 & ~$perm_mask)) ))
                l_auser="root"
                l_agroup="(root|gdm|gdm3)"
                file_test_fix
                ;;
            *.journal | *.journal~)
                perm_mask='0137'
                maxperm=$((printf '%o' $(( 0777 & ~$perm_mask)) ))
                l_rperms="u-x,g-wx,o-rwx"
        esac
    done
}

```

```

    l_auser="root"
    l_agroup="(root|systemd-journal)"
    file_test_fix
    ;;
*)
    perm_mask='0137'
    maxperm=$( printf '%o' $(( 0777 & ~$perm_mask)) )
    l_rperms="u~x,g-wx,o-rwx"
    l_auser="(root|syslog)"
    l_agroup="(root|adm)"
    if [ "$l_uid" -lt "$l_uidmin" ] && [ -z "$(awk -v grp="$l_group" -F: '$1==grp {print $4}' /etc/group)" ]; then
        if [[ ! "$l_user" =~ $l_auser ]]; then
            l_auser="(root|syslog|$l_user)"
        fi
        if [[ ! "$l_group" =~ $l_agroup ]]; then
            l_tst=""
            while l_out3=""; read -r l_duid; do
                [ "$l_duid" -ge "$l_uidmin" ] && l_tst=failed
            done <<< "$(awk -F: '$4=="$l_gid" {print $3}' /etc/passwd)"
            [ "$l_tst" != "failed" ] && l_agroup="(root|adm|$l_group)"
        fi
        fi
        file_test_fix
    ;;
    esac
done <<< "$(printf '%s\n' "${a_file[@]}")"
unset a_file # Clear array
# If all files passed, then we report no changes
if [ -z "$l_output2" ]; then
    echo -e "- All files in \"/var/log/\" have appropriate permissions and ownership\n - No
changes required\n"
else
    # print report of changes
    echo -e "\n$l_output2"
fi
}
}

```

**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.

## References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	M1028

## 6.4 System Auditing

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.
- 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 organization 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.

### **6.4.1 Configure auditd Service**

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

### *6.4.1.1 Ensure auditd packages are 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` is installed:

```
# dpkg-query -s auditd &>/dev/null && echo auditd is installed  
auditd is installed
```

Run the following command to verify `audispd-plugins` is installed:

```
# dpkg-query -s audispd-plugins &>/dev/null && echo audispd-plugins is  
installed  
audispd-plugins is installed
```

#### **Remediation:**

Run the following command to Install `auditd` and `audispd-plugins`

```
# apt install auditd audispd-plugins
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-3, AU-12, SI-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.5 Collect Detailed Audit Logs</b>  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><b>6.2 Activate audit logging</b>  Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	M1018

### *6.4.1.2 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 | grep '^enabled'  
enabled
```

Verify result is "enabled".

Run the following command to verify `auditd` is active:

```
# systemctl is-active auditd | grep '^active'  
active
```

Verify result is active

#### **Remediation:**

Run the following commands to unmask, enable and start `auditd`:

```
# systemctl unmask auditd  
# systemctl enable auditd  
# systemctl start auditd
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> 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	M1028

### *6.4.1.3 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
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-3, AU-12

#### **Additional Information:**

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

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.2 Collect Audit Logs</b>            Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b>            Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	M1047

#### *6.4.1.4 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`

##### **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-3, AU-12

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b> 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	M1028

## **6.4.2 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.

### *6.4.2.1 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
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-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	<p><b>8.3 Ensure Adequate Audit Log Storage</b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.</p>	●	●	●
v7	<p><b>6.4 Ensure adequate storage for logs</b> Ensure that all systems that store logs have adequate storage space for the logs generated.</p>		●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0040	M1053

## 6.4.2.2 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
```

### References:

1. NIST SP 800-53 Rev. 5: AU-8

### CIS Controls:

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

**MITRE ATT&CK Mappings:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1562, T1562.006	TA0005	M1053

### **6.4.2.3 Ensure system is disabled when audit logs are full (Automated)**

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The `audited` daemon can be configured to halt the system or put the system in single user mode, if no free space is available or an error is detected on the partition that holds the audit log files.

The `disk_full_action` parameter tells the system what action to take when no free space is available on the partition that holds the audit log files. Valid values are `ignore`, `syslog`, `rotate`, `exec`, `suspend`, `single`, and `halt`.

- `ignore`, the audit daemon will issue a syslog message but no other action is taken
- `syslog`, the audit daemon will issue a warning to syslog
- `rotate`, the audit daemon will rotate logs, losing the oldest to free up space
- `exec`, /path-to-script will execute the script. You cannot pass parameters to the script. The script is also responsible for telling the audited daemon to resume logging once its completed its action
- `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 shut down the system

The `disk_error_action` parameter tells the system what action to take when an error is detected on the partition that holds the audit log files. Valid values are `ignore`, `syslog`, `exec`, `suspend`, `single`, and `halt`.

- `ignore`, the audit daemon will not take any action
- `syslog`, the audit daemon will issue no more than 5 consecutive warnings to syslog
- `exec`, /path-to-script will execute the script. You cannot pass parameters to the script
- `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 shut down the system

#### **Rationale:**

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

## **Impact:**

`disk_full_action` parameter:

- Set to `halt` - the `auditd` daemon will shutdown the system when the disk partition containing the audit logs becomes full.
- Set to `single` - the `auditd` daemon will put the computer system in single user mode when the disk partition containing the audit logs becomes full.

`disk_error_action` parameter:

- Set to `halt` - the `auditd` daemon will shutdown the system when an error is detected on the partition that holds the audit log files.
- Set to `single` - the `auditd` daemon will put the computer system in single user mode when an error is detected on the partition that holds the audit log files.
- Set to `syslog` - the `auditd` daemon will issue no more than 5 consecutive warnings to `syslog` when an error is detected on the partition that holds the audit log files.

## **Audit:**

Run the following command and verify the `disk_full_action` is set to either `halt` or `single`:

```
# grep -Pi -- '^h*disk_full_action\h*=\h*(halt|single)\b'  
/etc/audit/auditd.conf  
  
disk_full_action = <halt|single>
```

Run the following command and verify the `disk_error_action` is set to `syslog`, `single`, or `halt`:

```
# grep -Pi -- '^h*disk_error_action\h*=\h*(syslog|single|halt)\b'  
/etc/audit/auditd.conf  
  
disk_error_action = <syslog|single|halt>
```

## **Remediation:**

Set one of the following parameters in `/etc/audit/auditd.conf` depending on your local security policies.

```
disk_full_action = <halt|single>
disk_error_action = <syslog|single|halt>
```

*Example:*

```
disk_full_action = halt
disk_error_action = halt
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-8, AU-12, SI-5
2. AUDITD.CONF(5)

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	<b>8.3 Ensure Adequate Audit Log Storage</b> 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	M1028

#### *6.4.2.4 Ensure system warns when audit logs are low on space (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

The `audited` daemon can be configured to halt the system, put the system in single user mode or send a warning message, if the partition that holds the audit log files is low on space.

The `space_left_action` parameter tells the system what action to take when the system has detected that it is starting to get low on disk space. Valid values are `ignore`, `syslog`, `rotate`, `email`, `exec`, `suspend`, `single`, and `halt`.

- `ignore`, the audit daemon does nothing
- `syslog`, the audit daemon will issue a warning to syslog
- `rotate`, the audit daemon will rotate logs, losing the oldest to free up space
- `email`, the audit daemon will send a warning to the email account specified in `action_mail_acct` as well as sending the message to syslog
- `exec`, `/path-to-script` will execute the script. You cannot pass parameters to the script. The script is also responsible for telling the audited daemon to resume logging once its completed its action
- `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 shut down the system

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`, `rotate`, `email`, `exec`, `suspend`, `single`, and `halt`.

- `ignore`, the audit daemon does nothing
- `syslog`, the audit daemon will issue a warning to syslog
- `rotate`, the audit daemon will rotate logs, losing the oldest to free up space
- `email`, the audit daemon will send a warning to the email account specified in `action_mail_acct` as well as sending the message to syslog
- `exec`, `/path-to-script` will execute the script. You cannot pass parameters to the script. The script is also responsible for telling the audited daemon to resume logging once its completed its action
- `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 shut down 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` is set to `single` the audit daemon will put the computer system in single user mode.

## Audit:

Run the following command and verify the `space_left_action` is set to `email`, `exec`, `single`, or `halt`:

```
grep -Pi -- '^h*space_left_action\h*=\h*(email|exec|single|halt)\b'  
/etc/audit/auditd.conf
```

Verify the output is `email`, `exec`, `single`, or `halt`

*Example output*

```
space_left_action = email
```

Run the following command and verify the `admin_space_left_action` is set to `single` - **OR** - `halt`:

```
grep -Pi -- '^h*admin_space_left_action\h*=\h*(single|halt)\b'  
/etc/audit/auditd.conf
```

Verify the output is `single` or `halt`

*Example output:*

```
admin_space_left_action = single
```

**Note:** A Mail Transfer Agent (MTA) must be installed and configured properly to set `space_left_action = email`

## Remediation:

Set the `space_left_action` parameter in `/etc/audit/auditd.conf` to `email`, `exec`, `single`, or `halt`:

*Example:*

```
space_left_action = email
```

Set the `admin_space_left_action` parameter in `/etc/audit/auditd.conf` to `single` or `halt`:

*Example:*

```
admin_space_left_action = single
```

**Note:** A Mail Transfer Agent (MTA) must be installed and configured properly to set `space_left_action = email`

## References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-8, AU-12, SI-5
2. AUDITD.CONF(5)

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	<b>8.3 Ensure Adequate Audit Log Storage</b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	<b>6.2 Activate audit logging</b> 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	TA0005	

### 6.4.3 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.

**Note:** The Linux Benchmarks are written and tested against x86\_64 processor architecture. If you are running a different processor type, please review and update the audit rules for the processor architecture of the system

### *6.4.3.1 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 '%s\n' "-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
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3

## **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 optimized for performance as per the man page.

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>4.8 Log and Alert on Changes to Administrative Group Membership</b> 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

### *6.4.3.2 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:

### 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
```

## **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.

*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
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-3

## **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 optimized for performance as per the man page.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.5 Collect Detailed Audit Logs</b>  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><b>4.9 Log and Alert on Unsuccessful Administrative Account Login</b>  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

### *6.4.3.3 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.

## Audit:

**Note:** This recommendation requires that the sudo logfile is configured. See guidance provided in the recommendation "Ensure sudo log file exists"

### On disk configuration

Run the following command to check the on disk rules:

```
# {
  SUDO_LOG_FILE=$(grep -r logfile /etc/sudoers* | sed -e 's/.*logfile=//;s/,?
.*//' -e 's/"//g' -e 's|/|\\||g')
  [ -n "${SUDO_LOG_FILE}" ] && awk "/^ *-w/ \
&&/"${SUDO_LOG_FILE}"/ \
&&/+-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/) " /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'SUDO_LOG_FILE' is unset.\n"
}
```

Verify output 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=$(grep -r logfile /etc/sudoers* | sed -e 's/.*logfile=//;s/,?
.*//' -e 's/"//g' -e 's|/|\\||g')
  [ -n "${SUDO_LOG_FILE}" ] && auditctl -l | awk "/^ *-w/ \
&&/"${SUDO_LOG_FILE}"/ \
&&/+-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/) " \
|| printf "ERROR: Variable 'SUDO_LOG_FILE' is unset.\n"
}
```

Verify output matches:

```
-w /var/log/sudo.log -p wa -k sudo_log_file
```

## **Remediation:**

**Note:** This recommendation requires that the sudo logfile is configured. See guidance provided in the recommendation "Ensure sudo log file exists"

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}" ] && printf "
-w ${SUDO_LOG_FILE} -p wa -k sudo_log_file
" >> /etc/audit/rules.d/50-sudo.rules || printf "ERROR: Variable 'SUDO_LOG_FILE' 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 optimized for performance as per the man page.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.5 <u>Collect Detailed Audit Logs</u></b>  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><b>4.9 <u>Log and Alert on Unsuccessful Administrative Account Login</u></b>  Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.</p>	●	●	●

#### *6.4.3.4 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_settime` - 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:

### 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_settime/ ) \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules

awk '/^ *-w/ \
&&(/etc/localtime/ \
&& +p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
}
```

Verify output of 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
```

## 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.

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
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3, CM-6

## 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 optimized for performance as per the man page.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.5 Collect Detailed Audit Logs</b>  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><b>5.5 Implement Automated Configuration Monitoring Systems</b>  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	TA0005	M1047

### *6.4.3.5 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
- `/etc/netplan/` - central location for YAML networking configurations files

#### **Rationale:**

Monitoring system events that change network environments, such as `sethostname` and `setdomainname`, helps identify unauthorized alterations to host and domain names, which could compromise security settings reliant on these names. Changes to `/etc/hosts` can signal unauthorized attempts to alter machine associations with IP addresses, potentially redirecting users and processes to unintended destinations. Surveillance of `/etc/issue` and `/etc/issue.net` is crucial to detect intruders inserting false information to deceive users. Monitoring `/etc/network/` reveals modifications to network interfaces or scripts that may jeopardize system availability or security. Additionally, tracking changes in the `/etc/netplan/` directory ensures swift detection of unauthorized adjustments to network configurations. All audit records should be appropriately tagged for relevance

## Audit:

### 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/ \
||/etc/netplan/) \
&& +-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
-w /etc/netplan -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/ \
||/etc/netplan/) \
&& +-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  
-w /etc/netplan -p wa -k system-locale
```

## 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.

*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  
-w /etc/netplan/ -p wa -k system-locale  
" >> /etc/audit/rules.d/50-system_locale.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
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3, CM-6
2. <https://netplan.io/faq>

## **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 optimized for performance as per the man page.

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>5.5 Implement Automated Configuration Monitoring Systems</b> 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	TA0003	M1047

### *6.4.3.6 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 script to check on disk rules:

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

{
    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 script to check loaded rules:

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

{
    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 script:*

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

{
    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}"
}
```

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.

## **References:**

1. NIST SP 800-53 Rev. 5: AU-3, AU-3(1)

## **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 optimized for performance as per the man page.

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>6.2 Activate audit logging</b> 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

### *6.4.3.7 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:

### 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
```

## 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 unsuccessful file access attempts.

*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
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3

## **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 optimized for performance as per the man page.

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</b> 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	M1047

#### *6.4.3.8 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
- /etc/nsswitch.conf - file configures how the system uses various databases and name resolution mechanisms
- /etc/pam.conf - file determines the authentication services to be used, and the order in which the services are used.
- /etc/pam.d - directory contains the PAM configuration files for each PAM-aware application.

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/ \
||/etc/nsswitch.conf/ \
||/etc/pam.conf/ \
||/etc/pam.d/) \
&&/ +-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
-w /etc/nsswitch.conf -p wa -k identity
-w /etc/pam.conf -p wa -k identity
-w /etc/pam.d -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/ \
||/etc/nsswitch.conf/ \
||/etc/pam.conf/ \
||/etc/pam.d/) \
&&/ +-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
-w /etc/nsswitch.conf -p wa -k identity
-w /etc/pam.conf -p wa -k identity
-w /etc/pam.d -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
-w /etc/nsswitch.conf -p wa -k identity
-w /etc/pam.conf -p wa -k identity
-w /etc/pam.d -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
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-3
2. <https://manpages.debian.org/bookworm/manpages/nsswitch.conf.5.en.html>
3. [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html/managing\\_smart\\_cards/pam\\_configuration\\_files](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/managing_smart_cards/pam_configuration_files)

## **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 optimized for performance as per the man page.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.5 Collect Detailed Audit Logs</b>  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><b>4.8 Log and Alert on Changes to Administrative Group Membership</b>  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

#### *6.4.3.9 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:

**Note:** Output showing all audited syscalls, e.g. (-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat,chmod,fchmod,fchmodat,setattr,lsetattr,fsetattr,removexattr,!removexattr,fremovexattr -F auid>=1000 -F auid!=unset -F key=perm\_mod) is also acceptable. These have been separated by function on the displayed output for clarity.

### 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>=${UID_MIN}/ \
  && (/chmod/||/fchmod/||/fchmodat/ \
    ||/chown/||/fchown/||/fchownat/||/lchown/ \
    ||/setattr/||/lsetattr/||/f setattr/ \
    ||/removexattr/||/lremovexattr/||/fremovexattr/) \
  && (/ key= *[!~-]* *$/||/ -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
setattr,lsetattr,f setattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S
setattr,lsetattr,f setattr,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

```

## **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.

*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
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-3, CM-6

## **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 optimized for performance as per the man page.

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>5.5 Implement Automated Configuration Monitoring Systems</b> 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

### *6.4.3.10 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:

### 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
```

## **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.

*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>=$UID_MIN -F auid!=unset -k
mounts
-a always,exit -F arch=b64 -S mount -F auid>=$UID_MIN -F auid!=unset -k
mounts
" >> /etc/audit/rules.d/50-mounts.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
```

## **References:**

1. NIST SP 800-53 Rev. 5: CM-6

## **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 optimized for performance as per the man page.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.5 Collect Detailed Audit Logs</b>  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><b>6.3 Enable Detailed Logging</b>  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	TA0010	M1034

### *6.4.3.11 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
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-3

## **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 optimized for performance as per the man page.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.5 Collect Detailed Audit Logs</b>  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><b>4.9 Log and Alert on Unsuccessful Administrative Account Login</b>  Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.</p>		●	●
v7	<p><b>16.13 Alert on Account Login Behavior Deviation</b>  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	M1047

### *6.4.3.12 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
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3

## **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 optimized for performance as per the man page.

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>8.5 Collect Detailed Audit Logs</u> 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	<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.		●	●
v7	<u>16.11 Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●
v7	<u>16.13 Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

### **MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0001	M1047

### *6.4.3.13 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:

### 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
```

## **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.

*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
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-12, SC-7

## **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 optimized for performance as per the man page.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.5 Collect Detailed Audit Logs</b>  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><b>6.2 Activate audit logging</b>  Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1047

#### *6.4.3.14 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
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3, CM-6

## **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 optimized for performance as per the man page.

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>5.5 Implement Automated Configuration Monitoring Systems</b> 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	TA0004	M1022

*6.4.3.15 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:**

The `chcon` command is used to change file security context. 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:

### 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
```

## **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.

*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
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

## **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 optimized for performance as per the man page.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.2 Collect Audit Logs</b>            Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b>            Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1022

*6.4.3.16 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:**

This utility sets Access Control Lists (ACLs) of files and directories. 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:

### 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
```

## **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.

*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-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
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

## **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 optimized for performance as per the man page.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.2 Collect Audit Logs</b>            Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b>            Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1022

*6.4.3.17 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.

`chacl` is an IRIX-compatibility command, and is maintained for those users who are familiar with its use from either XFS or IRIX.

**Rationale:**

`chacl` changes the ACL(s) for a file or directory. 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:

### 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 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>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/chacl/ \
    &&(/ key= *[!-~]* *$/|/ -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=perm_chng
```

## **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.

*Example:*

```
# {
  UID_MIN=$(awk '/^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
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

## **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 optimized for performance as per the man page.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.2 Collect Audit Logs</b>            Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b>            Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1022

*6.4.3.18 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:**

The `usermod` command modifies the system account files to reflect the changes that are specified on the command line. 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:

### 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
```

## **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.

*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
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

## **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 optimized for performance as per the man page.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.2 Collect Audit Logs</b>            Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b>            Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1022

### *6.4.3.19 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

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:

### 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/) \
&&(/ 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 -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/) \
&&(/ 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 init_module,delete_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=$(ls -l /usr/sbin/lsmod /usr/sbin/rmmod /usr/sbin/insmod
/usr/sbin/modinfo /usr/sbin/modprobe /usr/sbin/depmod | grep -vE " ->
(\.\./)?bin/kmod" || true) \
&& if [[ "${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.

### Example:

```
# {
UID_MIN=$(awk '/^UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S init_module,finit_module,delete_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
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3, CM-6

## **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 optimized for performance as per the man page.

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>6.2 Activate audit logging</b> 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	TA0004	M1047

#### *6.4.3.20 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 and verify output matches:

```
# grep -Ph -- '^\\h*-e\\h+2\\b' /etc/audit/rules.d/*.rules | tail -1  
-e 2
```

## **Remediation:**

Edit or create the file `/etc/audit/rules.d/99-finalize.rules` and add the line `-e 2` at the end of the file:

*Example:*

```
# printf -- "-e 2\n" >> /etc/audit/rules.d/99-finalize.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\nrequired to load rules\n"; fi
```

## **References:**

1. NIST SP 800-53 Rev. 5: AC-3, AU-3, AU-12, MP-2

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> 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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1562, T1562.001	TA0005	M1022

### *6.4.3.21 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
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-3

## **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:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

#### **6.4.4 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.

#### *6.4.4.1 Ensure audit log files mode is configured (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - 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 script to verify audit log files are mode 0640 or more restrictive:

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

{
    l_perm_mask="0137"
    if [ -e "/etc/audit/auditd.conf" ]; then
        l_audit_log_directory=$(dirname $(awk -F= '/^s*log_file\s*/{print $2}' /etc/audit/auditd.conf | xargs))"
        if [ -d "$l_audit_log_directory" ]; then
            l_maxperm=$((printf '%o' $(( 0777 & ~$l_perm_mask )) )"
            a_files=()
            while IFS= read -r -d $'\0' l_file; do
                [ -e "$l_file" ] && a_files+=("$l_file")
            done < <(find "$l_audit_log_directory" -maxdepth 1 -type f -perm /"$l_perm_mask" -print0)
            if (( "${#a_files[@]}" > 0 )); then
                for l_file in "${a_files[@]}"; do
                    l_file_mode=$(stat -Lc '%#a' "$l_file")
                    echo -e "\n- Audit Result:\n  ** FAIL **\n - File:
\"$l_file\" is mode: \"$l_file_mode\"\n      (should be mode: \"$l_maxperm\" or more restrictive)\n"
                done
            else
                echo -e "\n- Audit Result:\n  ** PASS **\n - All files in
\"$l_audit_log_directory\" are mode: \"$l_maxperm\" or more restrictive"
            fi
        else
            echo -e "\n- Audit Result:\n  ** FAIL **\n - Log file directory not set in \"/etc/audit/auditd.conf\" please set log file directory"
            fi
        else
            echo -e "\n- Audit Result:\n  ** FAIL **\n - File:
\"/etc/audit/auditd.conf\" not found.\n      - ** Verify auditd is installed **"
            fi
    }
}
```

## Remediation:

Run the following command to remove more permissive mode than 0640 from audit log files:

```
# [ -f /etc/audit/auditd.conf ] && find "$(dirname $(awk -F "=" '/^s*log_file/ {print $2}' /etc/audit/auditd.conf | xargs))" -type f -perm /0137 -exec chmod u-x,g-wx,o-rwx {} +
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	M1022

#### *6.4.4.2 Ensure audit log files owner is configured (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - 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 script to verify audit log files are owned by the `root` user:

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

{
    l_output="" l_output2=""
    if [ -e "/etc/audit/auditd.conf" ]; then
        l_audit_log_directory=$(dirname $(awk -F= '/^s*log_file\s*/{print $2}' /etc/audit/auditd.conf | xargs))"
        if [ -d "$l_audit_log_directory" ]; then
            while IFS= read -r -d '$\0' l_file; do
                l_output2="$l_output2\n - File: \"$l_file\" is owned by user:
\"$(stat -Lc '%U' \"$l_file\")\"\n      (should be owned by user: \"root\")\n"
            done <<(find "$l_audit_log_directory" -maxdepth 1 -type f ! -user root -print0)
        else
            l_output2="$l_output2\n - Log file directory not set in
\"/etc/audit/auditd.conf\" please set log file directory"
        fi
    else
        l_output2="$l_output2\n - File: \"/etc/audit/auditd.conf\" not
found.\n - ** Verify auditd is installed **"
    fi
    if [ -z "$l_output2" ]; then
        l_output="$l_output\n - All files in \"$l_audit_log_directory\" are
owned by user: \"root\"\n"
        echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured *
:$l_output"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :$l_output2\n"
    fi
}
```

## Remediation:

Run the following command to configure the audit log files to be owned by the `root` user:

```
# [ -f /etc/audit/auditd.conf ] && find "$(dirname $(awk -F= "="
'/^s*log_file/ {print $2}' /etc/audit/auditd.conf | xargs))" -type f ! -user
root -exec chown root {} +
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	M1022

### *6.4.4.3 Ensure audit log files group owner is configured (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - 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 -Piws -- '^h*log_group\h*=\h*\H+\b' /etc/audit/auditd.conf | grep -Pvi -- '(adm)'
```

Nothing should be returned

Using the path of the directory containing the audit logs, verify audit log files are owned by the "root" or "adm" group by running the following script:

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

{
    if [ -e /etc/audit/auditd.conf ]; then
        l_fpath=$(dirname "$(awk -F "=" '/^s*log_file/ {print $2}' /etc/audit/auditd.conf | xargs)"
        find -L "$l_fpath" -not -path "$l_fpath"/lost+found -type f \(! -group
root -a ! -group adm \) -exec ls -l {} +
    fi
}
```

Nothing should be returned

## Remediation:

Run the following command to configure the audit log files to be group owned by `adm`:

```
# find $(dirname $(awk -F"="/^\\s*log_file/ {print $2}")' /etc/audit/auditd.conf | xargs)) -type f \(! -group adm -a ! -group root \) -exec chgrp adm {} +
```

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*#.*)?.*$//g' /etc/audit/auditd.conf
```

Run the following command to restart the audit daemon to reload the configuration file:

```
# systemctl restart auditd
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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	M1022

#### *6.4.4.4 Ensure the audit log file directory mode is configured (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - 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 script to verify the audit log directory is mode 0750 or more restrictive:

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

{
    l_perm_mask="0027"
    if [ -e "/etc/audit/auditd.conf" ]; then
        l_audit_log_directory=$(dirname $(awk -F= '/^s*log_file\s*/{print $2}' /etc/audit/auditd.conf | xargs))"
        if [ -d "$l_audit_log_directory" ]; then
            l_maxperm=$(printf '%o' $(( 0777 & ~$l_perm_mask )) )
            l_directory_mode=$(stat -Lc '%#a' "$l_audit_log_directory")
            if [ $(( $l_directory_mode & $l_perm_mask )) -gt 0 ]; then
                echo -e "\n- Audit Result:\n ** FAIL **\n - Directory:
\"$l_audit_log_directory\" is mode: \"$l_directory_mode\"\n      (should be
mode: \"$l_maxperm\" or more restrictive)\n"
            else
                echo -e "\n- Audit Result:\n ** PASS **\n - Directory:
\"$l_audit_log_directory\" is mode: \"$l_directory_mode\"\n      (should be
mode: \"$l_maxperm\" or more restrictive)\n"
            fi
        else
            echo -e "\n- Audit Result:\n ** FAIL **\n - Log file directory not
set in \"/etc/audit/auditd.conf\" please set log file directory"
            fi
        else
            echo -e "\n- Audit Result:\n ** FAIL **\n - File:
\"/etc/audit/auditd.conf\" not found\n - ** Verify auditd is installed **"
            fi
    }
}
```

## 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 | xargs))"
```

## Default Value:

750

## References:

1. NIST SP 800-53 Rev. 5: AU-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	M1022

#### *6.4.4.5 Ensure audit configuration files mode is configured (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - 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 script to verify that the audit configuration files are mode 0640 or more restrictive:

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

{
    l_output="" l_output2="" l_perm_mask="0137"
    l_maxperm=$( printf '%o' $(( 0777 & ~$l_perm_mask )) )
    while IFS= read -r -d $'\0' l_fname; do
        l_mode=$(stat -Lc '%#a' "$l_fname")
        if [ $(( "$l_mode" & "$l_perm_mask" )) -gt 0 ]; then
            l_output2="$l_output2\n- file: \"$l_fname\" is mode: \"$l_mode\""
            (should be mode: \"$l_maxperm\" or more restrictive)"
        fi
    done < <(find /etc/audit/ -type f \(
        -name "*.conf" -o -name "*.rules" \
        -print0)
        if [ -z "$l_output2" ]; then
            echo -e "\n- Audit Result:\n  ** PASS **\n- All audit configuration
files are mode: \"$l_maxperm\" or more restrictive"
        else
            echo -e "\n- Audit Result:\n  ** FAIL **\n$l_output2"
        fi
    }
```

## 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 {} +
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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	M1022

## *6.4.4.6 Ensure audit configuration files owner is configured (Automated)*

### **Profile Applicability:**

- Level 2 - Server
- Level 2 - 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 are owned by the root user:

```
# 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 {} +
```

### **References:**

1. NIST SP 800-53 Rev. 5: AU-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	M1022

## *6.4.4.7 Ensure audit configuration files group owner is configured (Automated)*

### **Profile Applicability:**

- Level 2 - Server
- Level 2 - 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 are owned by the group `root`:

```
# 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 {} +
```

### **References:**

1. NIST SP 800-53 Rev. 5: AU-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	M1022

#### *6.4.4.8 Ensure audit tools mode is configured (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - 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 script to verify the audit tools are mode 0755 or more restrictive:

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

{
    l_output="" l_output2="" l_perm_mask="0022"
    l_maxperm=$(printf '%o' $(( 0777 & ~$l_perm_mask )) )
    a_audit_tools=("/sbin/auditctl" "/sbin/aureport" "/sbin/ausearch"
    "/sbin/autrace" "/sbin/auditd" "/sbin/augenrules")
    for l_audit_tool in "${a_audit_tools[@]}"; do
        l_mode=$(stat -Lc '%#a' "$l_audit_tool")
        if [ $(( ${l_mode} & ${l_perm_mask} )) -gt 0 ]; then
            l_output2="$l_output2\n - Audit tool \"$l_audit_tool\" is mode:
\"$l_mode\" and should be mode: \"$l_maxperm\" or more restrictive"
        else
            l_output="$l_output\n - Audit tool \"$l_audit_tool\" is correctly
configured to mode: \"$l_mode\""
        fi
    done
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured *\n:$l_output"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure *\n:$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n - * Correctly configured *\n:$l_output\n"
    fi
    unset a_audit_tools
}
```

## 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
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	M1022

#### *6.4.4.9 Ensure audit tools owner is configured (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - 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 are owned by the `root` user:

```
# stat -Lc "%n %U" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/augenrules | awk '$2 != "root" {print}'
```

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
```

##### **References:**

1. NIST SP 800-53 Rev. 5: AU-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	M1022

#### *6.4.4.10 Ensure audit tools group owner is configured (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - 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 are owned by the group `root`

```
# stat -Lc "%n %G" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/augenrules | awk '$2 != "root" {print}'
```

Nothing should be returned

##### **Remediation:**

Run the following command to change group ownership to the group `root`:

```
# chgrp root /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/augenrules
```

##### **References:**

1. NIST SP 800-53 Rev. 5: AU-3

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	M1022

## **7 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.

## **7.1 System File Permissions**

This section provides guidance on securing aspects of system files and directories.

## *7.1.1 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 to verify `/etc/passwd` is mode 644 or more restrictive, **Uid is 0/root and Gid is 0/root**:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: ( %g/ %G)'  /etc/passwd
Access: (0644/-rw-r--r--)  Uid: ( 0/ root)  Gid: ( 0/ root)
```

### **Remediation:**

Run the following commands to remove excess permissions, set owner, and set group on `/etc/passwd`:

```
# chmod u-x,go-wx /etc/passwd
# chown root:root /etc/passwd
```

### **Default Value:**

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

## *7.1.2 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 to verify `/etc/passwd-` is mode 644 or more restrictive, Uid is 0/root and Gid is 0/root:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: { %g/ %G)' /etc/passwd-
Access: (0644/-rw-r--r--)  Uid: ( 0/ root)  Gid: { 0/ root)
```

### **Remediation:**

Run the following commands to remove excess permissions, set owner, and set group on `/etc/passwd-`:

```
# chmod u-x,go-wx /etc/passwd-
# chown root:root /etc/passwd-
```

### **Default Value:**

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: { 0/ root)

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

### *7.1.3 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 to verify `/etc/group` is mode 644 or more restrictive, `Uid` is 0/root and `Gid` is 0/root:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: ( %g/ %G)' /etc/group
Access: (0644/-rw-r--r--)  Uid: ( 0/ root)  Gid: ( 0/ root)
```

#### **Remediation:**

Run the following commands to remove excess permissions, set owner, and set group on `/etc/group`:

```
# chmod u-x,go-wx /etc/group
# chown root:root /etc/group
```

#### **Default Value:**

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

#### **References:**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

## *7.1.4 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 to verify `/etc/group-` is mode 644 or more restrictive, `Uid is 0/root and Gid is 0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: ( %g/ %G)'  /etc/group-
Access: (0644/-rw-r--r--)  Uid: ( 0/ root)  Gid: ( 0/ root)
```

### **Remediation:**

Run the following commands to remove excess permissions, set owner, and set group on `/etc/group-`:

```
# chmod u-x,go-wx /etc/group-
# chown root:root /etc/group-
```

### **Default Value:**

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

## 7.1.5 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 to verify `/etc/shadow` is mode 640 or more restrictive, `Uid` is 0/root and `Gid` is 0/root or ({GID}/ shadow):

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: ( %g/ %G)'  /etc/shadow
```

### Example:

```
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:shadow /etc/shadow
-OR-
# chown root:root /etc/shadow
```

Run the following command to remove excess permissions from `/etc/shadow`:

```
# chmod u-x,g-wx,o-rwx /etc/shadow
```

### Default Value:

Access: (0640/-rw-r-----) Uid: ( 0/ root) Gid: ( 42/ shadow)

## References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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, T1222, T1222.002	TA0005	M1022

## *7.1.6 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 to verify `/etc/shadow-` is mode 640 or more restrictive, Uid is 0/root and Gid is 0/root or {GID}/shadow:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: ( %g/ %G)'  /etc/shadow-
```

### **Example:**

```
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:shadow /etc/shadow-
-OR-
# chown root:root /etc/shadow-
```

Run the following command to remove excess permissions form `/etc/shadow-`:

```
# chmod u-x,g-wx,o-rwx /etc/shadow-
```

### **Default Value:**

Access: (0640/-rw-r----) Uid: ( 0/ root) Gid: ( 42/ shadow)

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

## 7.1.7 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 to verify `/etc/gshadow` is mode 640 or more restrictive, Uid is 0/root and Gid is 0/root or `{:GID}/shadow:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: ( %g/ %G)'  /etc/gshadow
```

### Example:

```
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:shadow /etc/gshadow
-OR-
# chown root:root /etc/gshadow
```

Run the following command to remove excess permissions from `/etc/gshadow`:

```
# chmod u-x,g-wx,o-rwx /etc/gshadow
```

### Default Value:

Access: (0640/-rw-r-----) Uid: ( 0/ root) Gid: ( 42/ shadow)

## References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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, T1222, T1222.002	TA0005	M1022

## *7.1.8 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 to verify `/etc/gshadow-` is mode 640 or more restrictive, Uid is 0/root and Gid is 0/root or {GID}/shadow:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: ( %g/ %G)'  /etc/gshadow-
```

### **Example:**

```
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:shadow /etc/gshadow-
-OR-
# chown root:root /etc/gshadow-
```

Run the following command to remove excess permissions form `/etc/gshadow-:`

```
# chmod u-x,g-wx,o-rwx /etc/gshadow-
```

### **Default Value:**

Access: (0640/-rw-r----) Uid: ( 0/ root) Gid: ( 42/ shadow)

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

## *7.1.9 Ensure permissions on /etc/shells are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

/etc/shells is a text file which contains the full pathnames of valid login shells. This file is consulted by chsh and available to be queried by other programs.

### **Rationale:**

It is critical to ensure that the /etc/shells 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 to verify /etc/shells is mode 644 or more restrictive, Uid is 0/root and Gid is 0/root:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: ( %g/ %G)' /etc/shells
Access: (0644/-rw-r--r--)  Uid: ( 0/ root)  Gid: ( 0/ root)
```

### **Remediation:**

Run the following commands to remove excess permissions, set owner, and set group on /etc/shells:

```
# chmod u-x,go-wx /etc/shells
# chown root:root /etc/shells
```

### **Default Value:**

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

### **References:**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

## *7.1.10 Ensure permissions on /etc/security/opasswd are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

/etc/security/opasswd **and its backup** /etc/security/opasswd.old **hold user's previous passwords if pam\_unix or pam\_pwhistory is in use on the system**

### **Rationale:**

It is critical to ensure that /etc/security/opasswd 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 commands to verify /etc/security/opasswd **and** /etc/security/opasswd.old **are mode 600 or more restrictive, Uid is 0/root and Gid is 0/root if they exist:**

```
# [ -e "/etc/security/opasswd" ] && stat -Lc '%n Access: (%#a/%A) Uid: (%u/ %U) Gid: (%g/ %G)' /etc/security/opasswd  
  
/etc/security/opasswd Access: (0600/-rw-----) Uid: ( 0/ root) Gid: ( 0/ root)  
-OR-  
Nothing is returned  
# [ -e "/etc/security/opasswd.old" ] && stat -Lc '%n Access: (%#a/%A) Uid: (%u/ %U) Gid: (%g/ %G)' /etc/security/opasswd.old  
  
/etc/security/opasswd.old Access: (0600/-rw-----) Uid: ( 0/ root) Gid: ( 0/ root)  
-OR-  
Nothing is returned
```

## **Remediation:**

Run the following commands to remove excess permissions, set owner, and set group on /etc/security/opasswd and /etc/security/opasswd.old if they exist:

```
# [ -e "/etc/security/opasswd" ] && chmod u-x,go-rwx /etc/security/opasswd  
# [ -e "/etc/security/opasswd" ] && chown root:root /etc/security/opasswd  
# [ -e "/etc/security/opasswd.old" ] && chmod u-x,go-rwx  
/etc/security/opasswd.old  
# [ -e "/etc/security/opasswd.old" ] && chown root:root  
/etc/security/opasswd.old
```

## **Default Value:**

/etc/security/opasswd Access: (0600/-rw-----) Uid: ( 0/ root) Gid: ( 0/ root)

## **References:**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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, T1222, T1222.002	TA0005	M1022

## *7.1.11 Ensure world writable files and directories are secured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

World writable files are the least secure. 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. See the `chmod(2)` man page for more information.

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

### **Rationale:**

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.

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

### **Audit:**

Run the following script to verify:

- No world writable files exist
- No world writable directories without the sticky bit exist

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    l_smask='01000'
    a_file=() a_dir=() # Initialize arrays
    a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path
"*/containerd/*" -a ! -path "*/kubelet/pods/*" -a ! -path
"*/kubelet/plugins/*" -a ! -path "/sys/*" -a ! -path "/snap/*")
    while IFS= read -r l_mount; do
        while IFS= read -r -d $'\0' l_file; do
            if [ -e "$l_file" ]; then
                [ -f "$l_file" ] && a_file+=("$l_file") # Add WR files
                if [ -d "$l_file" ]; then # Add directories w/o sticky bit
                    l_mode=$(stat -Lc '%#a' "$l_file")
                    [ ! $(( $l_mode & $l_smask )) -gt 0 ] && a_dir+=("$l_file")
                fi
            fi
        done <<(find "$l_mount" -xdev \(\ "${a_path[@]}" \) \(\ -type f -o -type
d \) -perm -0002 -print0 2>/dev/null)
        done <<(findmnt -Dkern fstype,target | awk '$1 !~
/^$s*(nfs|proc|smb|vfat|iso9660|efivarfs|selinuxfs)/ && $2 !~
/^($run$|user$|tmp$|var$|tmp$)/{print $2}')
        if ! (( ${#a_file[@]} > 0 )); then
            l_output="$l_output\n - No world writable files exist on the local
filesystem."
        else
            l_output2="$l_output2\n - There are \"$(printf '%s' "${#a_file[@]}")\""
World writable files on the system.\n - The following is a list of World
writable files:\n$(printf '%s\n' "${a_file[@]}")\n - end of list\n"
        fi
        if ! (( ${#a_dir[@]} > 0 )); then
            l_output="$l_output\n - Sticky bit is set on world writable
directories on the local filesystem."
        else
            l_output2="$l_output2\n - There are \"$(printf '%s' "${#a_dir[@]}")\""
World writable directories without the sticky bit on the system.\n - The
following is a list of World writable directories without the sticky
bit:\n$(printf '%s\n' "${a_dir[@]}")\n - end of list\n"
        fi
        unset a_path; unset a_arr; unset a_file; unset a_dir # Remove arrays
        # If l_output2 is empty, we pass
        if [ -z "$l_output2" ]; then
            echo -e "\n- Audit Result:\n ** PASS **\n - * Correctly configured *
:$l_output\n"
        else
            echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit
failure * :$l_output2"
            [ -n "$l_output" ] && echo -e "- * Correctly configured *
:$l_output\n"
        fi
    }
}

```

**Note:** On systems with a large number of files and/or directories, this audit may be a long running process

## **Remediation:**

- World Writable Files:
  - It is recommended that write access is removed from other with the command (`chmod o-w <filename>`), but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.
- World Writable Directories:
  - Set the sticky bit on all world writable directories with the command (`chmod a+t <directory_name>`)

Run the following script to:

- Remove other write permission from any world writable files
- Add the sticky bit to all world writable directories

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

{
    l_smask='01000'
    a_file=(); a_dir=() # Initialize arrays
    a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path
"*/containerd/*" -a ! -path "*/kubelet/pods/*" -a ! -path
"*/kubelet/plugins/*" -a ! -path "/sys/*" -a ! -path "/snap/*")
    while IFS= read -r l_mount; do
        while IFS= read -r -d $'\0' l_file; do
            if [ -e "$l_file" ]; then
                l_mode=$(stat -Lc '%#a' "$l_file")
                if [ -f "$l_file" ]; then # Remove excess permissions from WW
files
                    echo -e " - File: \"$l_file\" is mode: \"$l_mode\"\n -"
removing write permission on \"$l_file\" from \"other\""
                    chmod o-w "$l_file"
                fi
                if [ -d "$l_file" ]; then # Add sticky bit
                    if [ ! $(( $l_mode & $l_smask )) -gt 0 ]; then
                        echo -e " - Directory: \"$l_file\" is mode: \"$l_mode\" and"
doesn't have the sticky bit set\n - Adding the sticky bit"
                        chmod a+t "$l_file"
                    fi
                fi
            fi
        done <<(find "$l_mount" -xdev \({ ${a_path[@]} \} \) \(
-type f -o -type
d \) -perm -0002 -print0 2> /dev/null)
        done <<(findmnt -Dkerno fstype,target | awk '$1 !~
/^$s*(nfs|proc|smb|vfat|iso9660|efivars|selinuxfs)/ && $2 !~
/^($run$|/user$|/tmp$|/var$|/tmp$) / {print $2}')
    }
```

## **References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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, T1222.002, T1548	TA0004, TA0005	M1022, M1028

### *7.1.12 Ensure no files or directories without an owner and a group exist (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Administrators may delete users or groups from the system and neglect to remove all files and/or directories owned by those users or groups.

#### **Rationale:**

A new user or group who is assigned a deleted user's user ID or group ID may then end up "owning" a deleted user or group's files, and thus have more access on the system than was intended.

#### **Audit:**

Run the following script to verify no unowned or ungrouped files or directories exist:

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_nouser=() a_nogroup=() # Initialize arrays
    a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path
"*/containerd/*" -a ! -path "*/kubelet/pods/*" -a ! -path
"*/kubelet/plugins/*" -a ! -path "*/sys/fs/cgroup/memory/*" -a ! -path
"/var/*/private/*")
    while IFS= read -r l_mount; do
        while IFS= read -r -d $'\0' l_file; do
            if [ -e "$l_file" ]; then
                while IFS=: read -r l_user l_group; do
                    [ "$l_user" = "UNKNOWN" ] && a_nouser+=("$l_file")
                    [ "$l_group" = "UNKNOWN" ] && a_nogroup+=("$l_file")
                done < <(stat -Lc '%U:%G' "$l_file")
            fi
            done < <(find "$l_mount" -xdev \(\ ${a_path[@]} \) \(\ -type f -o -type
d \) \(\ -nouser -o -nogroup \) -print0 2> /dev/null)
            done < <(findmnt -Dkern fs_type,target | awk '$1 !~
/^$s*(nfs|proc|smb|vfat|iso9660|efivarfs|selinuxfs)/ && $2 !~
/^$s*/user//){print $2}')
            if ! (( ${#a_nouser[@]} > 0 )); then
                l_output="$l_output\n - No files or directories without a owner exist
on the local filesystem."
            else
                l_output2="$l_output2\n - There are \"$(printf '%s'
"${#a_nouser[@]}")\" unowned files or directories on the system.\n - The
following is a list of unowned files and/or directories:\n$(printf '%s\n'
"${a_nouser[@]}")\n - end of list"
            fi
            if ! (( ${#a_nogroup[@]} > 0 )); then
                l_output="$l_output\n - No files or directories without a group exist
on the local filesystem."
            else
                l_output2="$l_output2\n - There are \"$(printf '%s'
"${#a_nogroup[@]}")\" ungrouped files or directories on the system.\n - The
following is a list of ungrouped files and/or directories:\n$(printf '%s\n'
"${a_nogroup[@]}")\n - end of list"
            fi
            unset a_path; unset a_arr ; unset a_nouser; unset a_nogroup # Remove
arrays
            if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass
                echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured *
:$l_output\n"
            else
                echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :$l_output2"
                [ -n "$l_output" ] && echo -e "\n- * Correctly configured *
:$l_output\n"
            fi
    }
}

```

**Note:** On systems with a large number of files and/or directories, this audit may be a long running process

## **Remediation:**

Remove or set ownership and group ownership of these files and/or directories to an active user on the system as appropriate.

## **References:**

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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	TA0007	M1022

### *7.1.13 Ensure SUID and SGID files are reviewed (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 or SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

#### **Rationale:**

There are valid reasons for SUID and 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 checksum than what from the package. This is an indication that the binary may have been replaced.

## Audit:

Run the following script to generate a list of SUID and SGID files:

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

{
    l_output="" l_output2=""
    a_suid=(); a_sgids=() # initialize arrays
    while IFS= read -r l_mount_point; do
        if ! grep -Pqs '^h*/run/usr\b' <<< "$l_mount_point" && ! grep -Pqs -
- '\bnoexec\b' <<< "$(findmnt -krn "$l_mount_point")"; then
            while IFS= read -r -d $'\0' l_file; do
                if [ -e "$l_file" ]; then
                    l_mode=$(stat -Lc '%#a' "$l_file")
                    [ $(($l_mode & 04000)) -gt 0 ] && a_suid+=("$l_file")
                    [ $(($l_mode & 02000)) -gt 0 ] && a_sgids+=("$l_file")
                fi
            done <<(find "$l_mount_point" -xdev -type f \(
                -perm -2000 -o -perm
                -4000 \) -print0 2>/dev/null)
            fi
        done <<< "$(findmnt -Derno target)"
        if ! (( ${#a_suid[@]} > 0 )); then
            l_output="$l_output\n - No executable SUID files exist on the system"
        else
            l_output2="$l_output2\n - List of \"$(printf '%s' "${#a_suid[@]}")\""
            SUID executable files:\n$(printf '%s\n' "${a_suid[@]}")\n - end of list -\n"
        fi
        if ! (( ${#a_sgids[@]} > 0 )); then
            l_output="$l_output\n - There are no SGID files exist on the system"
        else
            l_output2="$l_output2\n - List of \"$(printf '%s' "${#a_sgids[@]}")\""
            SGID executable files:\n$(printf '%s\n' "${a_sgids[@]}")\n - end of list -\n"
        fi
        [ -n "$l_output2" ] && l_output2="$l_output2\n- Review the preceding
        list(s) of SUID and/or SGID files to\n- ensure that no rogue programs have
        been introduced onto the system.\n"
        unset a_arr; unset a_suid; unset a_sgids # Remove arrays
        # If l_output2 is empty, Nothing to report
        if [ -z "$l_output2" ]; then
            echo -e "\n- Audit Result:\n$l_output\n"
        else
            echo -e "\n- Audit Result:\n$l_output2\n"
            [ -n "$l_output" ] && echo -e "$l_output\n"
        fi
    }
}
```

**Note:** on systems with a large number of files, this may be a long running process

## Remediation:

Ensure that no rogue SUID or 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.

## References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5, AC-3, MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<b>14.6 Protect Information through Access Control Lists</b> 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, T1548.001	TA0004	M1028

## 7.2 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.

## *7.2.1 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.

### **Note:**

- 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 "User: \"\$1\" is not set to shadowed\npasswords \"\$2\""}' /etc/passwd
```

### **Remediation:**

Run the following command to set accounts to use shadowed passwords and migrate passwords in `/etc/passwd` to `/etc/shadow`:

```
# pwconv
```

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.

## References:

1. NIST SP 800-53 Rev. 5: IA-5
2. PWCONV(8)

## Additional Information:

The `pwconv` command creates shadow from `passwd` and an optionally existing `shadow`.

- The `pwunconv` command creates `passwd` from `passwd` and `shadow` and then removes `shadow`.
- The `grpconv` command creates `gshadow` from `group` and an optionally existing `gshadow`.
- The `grpunconv` command creates `group` from `group` and `gshadow` and then removes `gshadow`.

These four programs all operate on the normal and shadow password and group files: `/etc/passwd`, `/etc/group`, `/etc/shadow`, and `/etc/gshadow`.

Each program acquires the necessary locks before conversion. `pwconv` and `grpconv` are similar. First, entries in the shadowed file which don't exist in the main file are removed. Then, shadowed entries which don't have 'x' as the password in the main file are updated. Any missing shadowed entries are added. Finally, passwords in the main file are replaced with 'x'. These programs can be used for initial conversion as well to update the shadowed file if the main file is edited by hand.

`pwconv` will use the values of `PASS_MIN_DAYS`, `PASS_MAX_DAYS`, and `PASS_WARN_AGE` from `/etc/login.defs` when adding new entries to `/etc/shadow`.

`pwunconv` and `grpunconv` are similar. Passwords in the main file are updated from the shadowed file. Entries which exist in the main file but not in the shadowed file are left alone. Finally, the shadowed file is removed. Some password aging information is lost by `pwunconv`. It will convert what it can.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 Encrypt Sensitive Data at Rest</b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>16.4 Encrypt or Hash all Authentication Credentials</b> Encrypt or hash with a salt all authentication credentials when stored.		●	●

**MITRE ATT&CK Mappings:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1003, T1003.008	TA0003	M1027

## *7.2.2 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.

### **References:**

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.2 Use Unique Passwords</b>            Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.</p>	●	●	●
v7	<p><b>4.4 Use Unique Passwords</b>            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>		●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0003	M1027

### *7.2.3 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 to verify all GIDs in `/etc/passwd` exist in `/etc/group`:

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

{
    a_passwd_group_gid=("$ awk -F: '{print $4}' /etc/passwd | sort -u")
    a_group_gid=("$ awk -F: '{print $3}' /etc/group | sort -u")
    a_passwd_group_diff=("$ printf '%s\n' "${a_group_gid[@]}"
"${a_passwd_group_gid[@]}" | sort | uniq -u")
    while IFS= read -r l_gid; do
        awk -F: '$4 == "'$l_gid'" {print " - User: \\"$1 "\\ has GID: \\"$4 \\
which does not exist in /etc/group"}' /etc/passwd
        done << (printf '%s\n' "${a_passwd_group_diff[@]}")
        unset a_passwd_group_gid; unset a_group_gid; unset a_passwd_group_diff
}
```

Nothing should be returned

#### **Remediation:**

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

#### **References:**

1. 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><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Train Workforce Members on Recognizing and Reporting Security Incidents</b>  Train workforce members to be able to recognize a potential incident and be able to report such an incident.</p>	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0003	M1027

## 7.2.4 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: '$4 == "'$(getent group shadow | awk -F: '{print $3}' | xargs)''
{print " - user: """ $1 """ primary group is the shadow group"}' /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>
```

### References:

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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
T1003, T1003.008	TA0005	M1022

## 7.2.5 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:

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

{
    while read -r l_count l_uid; do
        if [ "$l_count" -gt 1 ]; then
            echo -e "Duplicate UID: \"$l_uid\" Users: \"$(awk -F: '($3 == n) {
print $1 }' n=$l_uid /etc/passwd | xargs)\""
        fi
    done < <(cut -f3 -d":" /etc/passwd | sort -n | uniq -c)
}
```

### 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.

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

### MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0005	M1027

## 7.2.6 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:

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

{
    while read -r l_count l_gid; do
        if [ "$l_count" -gt 1 ]; then
            echo -e "Duplicate GID: \"$l_gid\" Groups: \"$(awk -F: '($3 == n) {
print $1 }' n=$l_gid /etc/group | xargs)\""
        fi
    done < <(cut -f3 -d":" /etc/group | sort -n | uniq -c)
}
```

### 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.

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

### Additional Information:

You can also use the `grpck` command to check for other inconsistencies in the `/etc/group` file.

**MITRE ATT&CK Mappings:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1078, T1078.001, T1078.003	TA0005	M1027

## 7.2.7 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:

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

{
    while read -r l_count l_user; do
        if [ "$l_count" -gt 1 ]; then
            echo -e "Duplicate User: \"$l_user\" Users: \"$(awk -F: '($1 == n) { print $1 }' n=$l_user /etc/passwd | xargs)\""
            fi
        done < <(cut -f1 -d":" /etc/group | sort -n | uniq -c)
    }
```

### 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.

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**MITRE ATT&CK Mappings:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1078, T1078.001, T1078.003	TA0004	M1027

## 7.2.8 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:

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

{
    while read -r l_count l_group; do
        if [ "$l_count" -gt 1 ]; then
            echo -e "Duplicate Group: \"$l_group\" Groups: \"$(awk -F: '($1 == n) { print $1 }' n=$l_group /etc/group | xargs)\""
        fi
    done <<(cut -f1 -d":" /etc/group | sort -n | uniq -c)
}
```

### 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.

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**MITRE ATT&CK Mappings:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1078, T1078.001, T1078.003	TA0004	M1027

## *7.2.9 Ensure local interactive user home directories are configured (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. While the system administrator can establish secure permissions for users' home directories, the users can easily override these. Users can be defined in `/etc/passwd` without a home directory or with a home directory that does not actually exist.

### **Rationale:**

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory. 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. 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 Ensure:

- local interactive user home directories exist
- Ensure local interactive users own their home directories
- Ensure local interactive user home directories are mode 750 or more restrictive

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_heout2="" l_hoout2="" l_haout2=""
    l_valid_shells="^$( awk -F'\|' '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^//{s,,\\\,\,g;p}' | paste -s -d '|')$"
    unset a_uarr && a_uarr=() # Clear and initialize array
    while read -r l_epu l_eph; do # Populate array with users and user home
location
        a_uarr+=("{$l_epu $l_eph}")
    done <<< "$ awk -v pat=\"${l_valid_shells}\" -F: '$(NF) ~ pat { print $1 \" "
$(NF-1) }' /etc/passwd"
    l_asize="${#a_uarr[@]}" # Here if we want to look at number of users
before proceeding
    [ "${l_asize}" -gt "10000" ] && echo -e "\n ** INFO **\n - \"${l_asize}\"
Local interactive users found on the system\n - This may be a long running
check\n"
    while read -r l_user l_home; do
        if [ -d "${l_home}" ]; then
            l_mask='0027'
            l_max="$( printf '%o' $(( 0777 & ~$l_mask)) )"
            while read -r l_own l_mode; do
                [ "${l_user}" != "${l_own}" ] && l_hoout2="${l_hoout2}\n - User:
\"${l_user}\" Home \"${l_home}\" is owned by: \"${l_own}\""
                if [ $(($l_mode & $l_mask)) -gt 0 ]; then
                    l_haout2="${l_haout2}\n - User: \"${l_user}\" Home \"${l_home}\" is
mode: \"${l_mode}\" should be mode: \"${l_max}\" or more restrictive"
                fi
            done <<< "$(stat -Lc '%U %#a' "${l_home}")"
        else
            l_heout2="${l_heout2}\n - User: \"${l_user}\" Home \"${l_home}\" Doesn't
exist"
        fi
    done <<< "$(printf '%s\n' "${a_uarr[@]}")"
    [ -z "${l_heout2}" ] && l_output="${l_output}\n - home directories exist" ||
l_output2="${l_output} ${l_heout2}"
    [ -z "${l_hoout2}" ] && l_output="${l_output}\n - own their home directory" ||
l_output2="${l_output} ${l_hoout2}"
    [ -z "${l_haout2}" ] && l_output="${l_output}\n - home directories are mode:
\"${l_max}\" or more restrictive" || l_output2="${l_output} ${l_haout2}"
    [ -n "${l_output}" ] && l_output=" - All local interactive users:${l_output}"
    if [ -z "${l_output2}" ]; then # If l_output2 is empty, we pass
        echo -e "\n- Audit Result:\n ** PASS **\n - * Correctly configured *
:n${l_output}"
    else
        echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit
failure * :n${l_output2}"
        [ -n "${l_output}" ] && echo -e "\n- * Correctly configured *
:n${l_output}"
    fi
}

```

**Remediation:**

If a local interactive users' home directory is undefined and/or doesn't exist, follow local site policy and perform one of the following:

- Lock the user account
- Remove the user from the system
- create a directory for the user. If undefined, edit `/etc/passwd` and add the absolute path to the directory to the last field of the user.

Run the following script to:

- Remove excessive permissions from local interactive users home directories
- Update the home directory's owner

```

#!/usr/bin/env bash

{
    l_output2=""
    l_valid_shells="^( $( awk -F \/ '$NF != "nologin" {print}' /etc/shells | sed -rn '/^//{s,/,\\\/,g;p}' | paste -s -d '|') )$"
    unset a_uarr && a_uarr=() # Clear and initialize array
    while read -r l_epu l_eph; do # Populate array with users and user home location
        a_uarr+=("{$l_epu $l_eph}")
    done <<< "$ awk -v pat=\"${l_valid_shells}\" -F: '$(NF) ~ pat { print $1 \" \" $(NF-1) }' /etc/passwd"
    l_asize="${#a_uarr[@]}" # Here if we want to look at number of users before proceeding
    [ "${l_asize}" -gt "10000" ] && echo -e "\n ** INFO **\n - \"${l_asize}\"\n Local interactive users found on the system\n - This may be a long running process\n"
    while read -r l_user l_home; do
        if [ -d "${l_home}" ]; then
            l_mask='0027'
            l_max=$( printf '%o' $(( 0777 & ~$l_mask)) )
            while read -r l_own l_mode; do
                if [ "${l_user}" != "${l_own}" ]; then
                    l_output2="${l_output2}\n - User: \"${l_user}\" Home \"${l_home}\" is owned by: \"${l_own}\n - changing ownership to: \"${l_user}\n"
                    chown "${l_user}" "${l_home}"
                fi
                if [ $(( ${l_mode} & ${l_mask} )) -gt 0 ]; then
                    l_output2="${l_output2}\n - User: \"${l_user}\" Home \"${l_home}\" is mode: \"${l_mode}\" should be mode: \"${l_max}\" or more restrictive\n - removing excess permissions\n"
                    chmod g-w,o-rwx "${l_home}"
                fi
            done <<< "$(stat -Lc '%U %#a' "${l_home}")"
        else
            l_output2="${l_output2}\n - User: \"${l_user}\" Home \"${l_home}\" Doesn't exist\n - Please create a home in accordance with local site policy"
        fi
    done <<< "$(printf '%s\n' "${a_uarr[@]}")"
    if [ -z "${l_output2}" ]; then # If l_output2 is empty, we pass
        echo -e "\n - No modification needed to local interactive users home directories"
    else
        echo -e "\n${l_output2}"
    fi
}

```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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, T1222.002	TA0005	M1022

## *7.2.10 Ensure local interactive user dot files access is configured (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.

- `.forward` file specifies an email address to forward the user's mail to.
- `.rhost` file provides the "remote authentication" database for the rcp, rlogin, and rsh commands and the rcmd() function. These files bypass the standard password-based user authentication mechanism. They specify remote hosts and users that are considered trusted (i.e. are allowed to access the local system without supplying a password)
- `.netrc` file contains data for logging into a remote host or passing authentication to an API.
- `.bash_history` file keeps track of the user's commands.

### **Rationale:**

User configuration files with excessive or incorrect access 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:

- Don't include `.forward`, `.rhost`, or `.netrc` files
- Are mode 0644 or more restrictive
- Are owned by the local interactive user
- Are group owned by the user's primary group
- `.bash_history` is mode 0600 or more restrictive

**Note:** If a `.netrc` file is required, and follows local site policy, it should be mode 0600 or more restrictive.

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3=""
    l_bf="" l_df="" l_nf="" l_hf=""
    l_valid_shells="^$( awk -F\" '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^//{s,,\\\,\,g;p}' | paste -s -d '|\' - ))$"
    unset a_uarr && a_uarr=() # Clear and initialize array
    while read -r l_epu l_eph; do # Populate array with users and user home
location
        [[ -n "$l_epu" && -n "$l_eph" ]] && a_uarr+=("$l_epu $l_eph")
        done <<< "$ awk -v pat=\"$l_valid_shells\" -F: '$(NF) ~ pat { print $1 \" "
$ (NF-1) }' /etc/passwd"
    l_asize="${#a_uarr[@]}" # Here if we want to look at number of users
before proceeding
    l_maxsize="1000" # Maximun number of local interactive users before
warning (Default 1,000)
    [ "$l_asize " -gt "$l_maxsize" ] && echo -e "\n ** INFO **\n -
\"$l_asize\" Local interactive users found on the system\n - This may be a
long running check\n"
    file_access_chk()
    {
        l_facout2=""
        l_max=$( printf '%o' $(( 0777 & ~$l_mask)) )
        if [ $(( $l_mode & $l_mask )) -gt 0 ]; then
            l_facout2="$l_facout2\n - File: \"$l_hdfile\" is mode: \"$l_mode\""
and should be mode: \"$l_max\" or more restrictive"
            fi
        if [[ ! "$l_owner" =~ ($l_user) ]]; then
            l_facout2="$l_facout2\n - File: \"$l_hdfile\" owned by:
\"$l_owner\" and should be owned by \"${l_user//|/ or }\""
            fi
        if [[ ! "$l_gowner" =~ ($l_group) ]]; then
            l_facout2="$l_facout2\n - File: \"$l_hdfile\" group owned by:
\"$l_gowner\" and should be group owned by \"${l_group//|/ or }\""
            fi
        }
        while read -r l_user l_home; do
            l_fe="" l_nout2="" l_nout3="" l_dfout2="" l_hdout2="" l_bhout2=""
            if [ -d "$l_home" ]; then
                l_group=$(id -gn "$l_user" | xargs)"
                l_group="${l_group// /|}"
                while IFS= read -r -d $'\0' l_hdfile; do
                    while read -r l_mode l_owner l_gowner; do
                        case "$(basename "$l_hdfile")" in
                            .forward | .rhost )
                                l_fe="Y" && l_bf="Y"
                                l_dfout2="$l_dfout2\n - File: \"$l_hdfile\" exists" ;;
                            .netrc )
                                l_mask='0177'
                                file_access_chk
                                if [ -n "$l_facout2" ]; then
                                    l_fe="Y" && l_nf="Y"
                                    l_nout2="$l_facout2"
                                else
                                    l_nout3=" - File: \"$l_hdfile\" exists"
                                fi ;;
                        esac
                done
            done
        done
    }
}

```

```

.bash_history )
    l_mask='0177'
    file_access_chk
    if [ -n "$l_facout2" ]; then
        l_fe="Y" && l_hf="Y"
        l_bhout2="$l_facout2"
    fi ;;
* )
    l_mask='0133'
    file_access_chk
    if [ -n "$l_facout2" ]; then
        l_fe="Y" && l_df="Y"
        l_hdout2="$l_facout2"
    fi ;;
esac
done <<< "$(stat -Lc '%#a %U %G' "$l_hdfile")"
done < <(find "$l_home" -xdev -type f -name '.*' -print0)
fi
if [ "$l_fe" = "Y" ]; then
    l_output2="$l_output2\n - User: \"$l_user\" Home Directory:
\"$l_home\""
    [ -n "$l_dfout2" ] && l_output2="$l_output2$l_dfout2"
    [ -n "$l_nout2" ] && l_output2="$l_output2$l_nout2"
    [ -n "$l_bhout2" ] && l_output2="$l_output2$l_bhout2"
    [ -n "$l_hdout2" ] && l_output2="$l_output2$l_hdout2"
fi
[ -n "$l_nout3" ] && l_output3="$l_output3\n - User: \"$l_user\" Home
Directory: \"$l_home\"\n$l_nout3"
done <<< "$(printf '%s\n' "${a_uarr[@]}")"
unset a_uarr # Remove array
[ -n "$l_output3" ] && l_output3=" - ** Warning **\n - \".netrc\" files
should be removed unless deemed necessary\n and in accordance with local
site policy:$l_output3"
[ -z "$l_bf" ] && l_output="$l_output\n - \".forward\" or \".rhost\"
files"
[ -z "$l_nf" ] && l_output="$l_output\n - \".netrc\" files with
incorrect access configured"
[ -z "$l_hf" ] && l_output="$l_output\n - \".bash_history\" files with
incorrect access configured"
[ -z "$l_df" ] && l_output="$l_output\n - \"dot\" files with incorrect
access configured"
[ -n "$l_output" ] && l_output=" - No local interactive users home
directories contain:$l_output"
if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass
    echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured *
:$l_output\n"
    echo -e "$l_output3\n"
else
    echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :\n$l_output2\n"
    echo -e "$l_output3\n"
    [ -n "$l_output" ] && echo -e "- * Correctly configured *
:$l_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 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
- change ownership of `dot` files within interactive users' home directories to the user
- change group ownership of `dot` files within interactive users' home directories to the user's primary group
- list `.forward` and `.rhost` files to be investigated and manually deleted

```

#!/usr/bin/env bash

{
    l_valid_shells="^( $( awk -F'/' '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^//{s,/,\\\/,g;p}' | paste -s -d '|') )$"
    unset a_uarr && a_uarr=() # Clear and initialize array
    while read -r l_epu l_eph; do # Populate array with users and user home
location
        [[ -n "$l_epu" && -n "$l_eph" ]] && a_uarr+=("$l_epu $l_eph")
done <<< "$ awk -v pat=\"$l_valid_shells\" -F: '$(NF) ~ pat { print $1 \" "
$(NF-1) }' /etc/passwd"
    l_asize="${#a_uarr[@]}" # Here if we want to look at number of users
before proceeding
    l_maxsize="1000" # Maximum number of local interactive users before
warning (Default 1,000)
    [ "$l_asize" -gt "$l_maxsize" ] && echo -e "\n ** INFO **\n -
\"$l_asize\" Local interactive users found on the system\n - This may be a
long running check\n"
    file_access_fix()
{
    l_facout2=""
    l_max=$( printf '%o' $(( 0777 & ~$l_mask)) )
    if [ $(( $l_mode & $l_mask )) -gt 0 ]; then
        echo -e "\n - File: \"$l_hdfile\" is mode: \"$l_mode\" and should be
mode: \"$l_max\" or more restrictive\n - Changing to mode \"$l_max\""
        chmod "$l_chp" "$l_hdfile"
    fi
    if [[ ! "$l_owner" =~ ($l_user) ]]; then
        echo -e "\n - File: \"$l_hdfile\" owned by: \"$l_owner\" and should
be owned by \"$l_user//|/ or }\\""\n - Changing ownership to \"$l_user\""
        chown "$l_user" "$l_hdfile"
    fi
    if [[ ! "$l_gowner" =~ ($l_group) ]]; then
        echo -e "\n - File: \"$l_hdfile\" group owned by: \"$l_gowner\" and
should be group owned by \"$l_group//|/ or }\\""\n - Changing group
ownership to \"$l_group\""
        chgrp "$l_group" "$l_hdfile"
    fi
}
    while read -r l_user l_home; do
        if [ -d "$l_home" ]; then
            echo -e "\n - Checking user: \"$l_user\" home directory:
\"$l_home\""
            l_group=$(id -gn "$l_user" | xargs)
            l_group="${l_group// /|}"
            while IFS= read -r -d $'\0' l_hdfile; do
                while read -r l_mode l_owner l_gowner; do
                    case "$(basename "$l_hdfile")" in
                        .forward | .rhost )
                            echo -e "\n - File: \"$l_hdfile\" exists\n - Please
investigate and manually delete \"$l_hdfile\""
                        ;;
                        .netrc )
                            l_mask='0177'
                            l_chp="u-x,go-rwx"
                            file_access_fix ;;
                        .bash_history )

```

```

        l_mask='0177'
        l_chp="u-x,go-rwx"
        file_access_fix ;;
    * )
        l_mask='0133'
        l_chp="u-x,go-wx"
        file_access_fix ;;
    esac
done <<< "$(stat -Lc '%#a %U %G' "$l_hdfile")"
done < <(find "$l_home" -xdev -type f -name '.*' -print0)
fi
done <<< "$(printf '%s\n' "${a_uarr[@]}")"
unset a_uarr # Remove array
}

```

## References:

1. 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><b>3.3 Configure Data Access Control Lists</b>  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><b>14.6 Protect Information through Access Control Lists</b>  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	<b>Initial Setup</b>		
1.1	<b>Filesystem</b>		
1.1.1	<b>Configure Filesystem Kernel Modules</b>		
1.1.1.1	Ensure cramfs kernel module is not available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure freevxfs kernel module is not available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure hfs kernel module is not available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure hfsplus kernel module is not available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.5	Ensure jffs2 kernel module is not available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.6	Ensure squashfs kernel module is not available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.7	Ensure udf kernel module is not available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.8	Ensure usb-storage kernel module is not available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	<b>Configure Filesystem Partitions</b>		
1.1.2.1	<b>Configure /tmp</b>		
1.1.2.1.1	Ensure /tmp is a separate partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.2	Ensure nodev option set on /tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.3	Ensure nosuid option set on /tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.4	Ensure noexec option set on /tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
<b>1.1.2.2</b>	<b>Configure /dev/shm</b>		
1.1.2.2.1	Ensure /dev/shm is a separate partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.2	Ensure nodev option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.4	Ensure noexec option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.1.2.3</b>	<b>Configure /home</b>		
1.1.2.3.1	Ensure separate partition exists for /home (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.2	Ensure nodev option set on /home partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.3	Ensure nosuid option set on /home partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.1.2.4</b>	<b>Configure /var</b>		
1.1.2.4.1	Ensure separate partition exists for /var (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.2	Ensure nodev option set on /var partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.3	Ensure nosuid option set on /var partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.1.2.5</b>	<b>Configure /var/tmp</b>		
1.1.2.5.1	Ensure separate partition exists for /var/tmp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.2	Ensure nodev option set on /var/tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.4	Ensure noexec option set on /var/tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
<b>1.1.2.6</b>	<b>Configure /var/log</b>		
1.1.2.6.1	Ensure separate partition exists for /var/log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.2	Ensure nodev option set on /var/log partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.3	Ensure nosuid option set on /var/log partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.4	Ensure noexec option set on /var/log partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.1.2.7</b>	<b>Configure /var/log/audit</b>		
1.1.2.7.1	Ensure separate partition exists for /var/log/audit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.2</b>	<b>Package Management</b>		
<b>1.2.1</b>	<b>Configure Package Repositories</b>		
1.2.1.1	Ensure GPG keys are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.2	Ensure package manager repositories are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.2.2</b>	<b>Configure Package Updates</b>		
1.2.2.1	Ensure updates, patches, and additional security software are installed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.3</b>	<b>Mandatory Access Control</b>		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.3.1	<b>Configure AppArmor</b>		
1.3.1.1	Ensure AppArmor is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.2	Ensure AppArmor is enabled in the bootloader configuration (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.3	Ensure all AppArmor Profiles are in enforce or complain mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.4	Ensure all AppArmor Profiles are enforcing (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	<b>Configure Bootloader</b>		
1.4.1	Ensure bootloader password is set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure access to bootloader config is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	<b>Configure Additional Process Hardening</b>		
1.5.1	Ensure address space layout randomization is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure ptrace_scope is restricted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Ensure core dumps are restricted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Ensure prelink is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Ensure Automatic Error Reporting is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6	<b>Configure Command Line Warning Banners</b>		
1.6.1	Ensure message of the day is configured properly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.2	Ensure local login warning banner is configured properly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.6.3	Ensure remote login warning banner is configured properly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure access to /etc/motd is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure access to /etc/issue is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure access to /etc/issue.net is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.7</b>	<b>Configure GNOME Display Manager</b>		
1.7.1	Ensure GDM is removed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.2	Ensure GDM login banner is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.3	Ensure GDM disable-user-list option is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.4	Ensure GDM screen locks when the user is idle (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.5	Ensure GDM screen locks cannot be overridden (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.6	Ensure GDM automatic mounting of removable media is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.7	Ensure GDM disabling automatic mounting of removable media is not overridden (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.8	Ensure GDM autorun-never is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.9	Ensure GDM autorun-never is not overridden (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7.10	Ensure XDCMP is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2</b>	<b>Services</b>		
<b>2.1</b>	<b>Configure Server Services</b>		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure autofs services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure avahi daemon services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure dhcp server services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Ensure dns server services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Ensure dnsmasq services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure ftp server services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Ensure ldap server services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Ensure message access server services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Ensure network file system services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.10	Ensure nis server services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.11	Ensure print server services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure rpcbind services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.13	Ensure rsync services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure samba file server services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.15	Ensure snmp services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.16	Ensure tftp server services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.17	Ensure web proxy server services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.18	Ensure web server services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.19	Ensure xinetd services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.20	Ensure X window server services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.21	Ensure mail transfer agent is configured for local-only mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.22	Ensure only approved services are listening on a network interface (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.2</b>	<b>Configure Client Services</b>		
2.2.1	Ensure NIS Client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure rsh client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure talk client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure telnet client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure ldap client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure ftp client is not installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.3</b>	<b>Configure Time Synchronization</b>		
<b>2.3.1</b>	<b>Ensure time synchronization is in use</b>		
2.3.1.1	Ensure a single time synchronization daemon is in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.3.2</b>	<b>Configure systemd-timesyncd</b>		
2.3.2.1	Ensure systemd-timesyncd configured with authorized timeserver (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2	Ensure systemd-timesyncd is enabled and running (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.3.3</b>	<b>Configure chrony</b>		
2.3.3.1	Ensure chrony is configured with authorized timeserver (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.3.2	Ensure chrony is running as user _chrony (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3	Ensure chrony is enabled and running (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.4</b>	<b>Job Schedulers</b>		
<b>2.4.1</b>	<b>Configure cron</b>		
2.4.1.1	Ensure cron daemon is enabled and active (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.2	Ensure permissions on /etc/crontab are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.3	Ensure permissions on /etc/cron.hourly are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.4	Ensure permissions on /etc/cron.daily are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.5	Ensure permissions on /etc/cron.weekly are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.6	Ensure permissions on /etc/cron.monthly are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.7	Ensure permissions on /etc/cron.d are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.8	Ensure crontab is restricted to authorized users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.4.2</b>	<b>Configure at</b>		
2.4.2.1	Ensure at is restricted to authorized users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3</b>	<b>Network</b>		
<b>3.1</b>	<b>Configure Network Devices</b>		
3.1.1	Ensure IPv6 status is identified (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure wireless interfaces are disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.3	Ensure bluetooth services are not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3.2</b>	<b>Configure Network Kernel Modules</b>		
3.2.1	Ensure dccp kernel module is not available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure tipc kernel module is not available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure rds kernel module is not available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure sctp kernel module is not available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3.3</b>	<b>Configure Network Kernel Parameters</b>		
3.3.1	Ensure ip forwarding is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure packet redirect sending is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure bogus icmp responses are ignored (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure broadcast icmp requests are ignored (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure icmp redirects are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure secure icmp redirects are not accepted (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 source routed packets are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure suspicious packets are logged (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.10	Ensure tcp syn cookies is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.11	Ensure ipv6 router advertisements are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4</b>	<b>Host Based Firewall</b>		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1	<b>Configure UncomplicatedFirewall</b>		
4.1.1	Ensure ufw is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure iptables-persistent is not installed with ufw (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure ufw service is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure ufw loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure ufw outbound connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure ufw firewall rules exist for all open ports (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure ufw default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2	<b>Configure nftables</b>		
4.2.1	Ensure nftables is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	Ensure ufw is uninstalled or disabled with nftables (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure iptables are flushed with nftables (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	Ensure a nftables table exists (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.5	Ensure nftables base chains exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.6	Ensure nftables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.7	Ensure nftables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.8	Ensure nftables default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.9	Ensure nftables service is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.2.10	Ensure nftables rules are permanent (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4.3</b>	<b>Configure iptables</b>		
<b>4.3.1</b>	<b>Configure iptables software</b>		
4.3.1.1	Ensure iptables packages are installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.2	Ensure nftables is not installed with iptables (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.3	Ensure ufw is uninstalled or disabled with iptables (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4.3.2</b>	<b>Configure IPv4 iptables</b>		
4.3.2.1	Ensure iptables default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.2	Ensure iptables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.3	Ensure iptables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.4	Ensure iptables firewall rules exist for all open ports (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4.3.3</b>	<b>Configure IPv6 ip6tables</b>		
4.3.3.1	Ensure ip6tables default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.2	Ensure ip6tables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.3	Ensure ip6tables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.4	Ensure ip6tables firewall rules exist for all open ports (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5</b>	<b>Access Control</b>		
<b>5.1</b>	<b>Configure SSH Server</b>		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure permissions on SSH private host key files are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on SSH public host key files are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure sshd access is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure sshd Banner is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure sshd Ciphers are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.8	Ensure sshd DisableForwarding is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.9	Ensure sshd GSSAPIAuthentication is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.10	Ensure sshd HostbasedAuthentication is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.11	Ensure sshd IgnoreRhosts is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.12	Ensure sshd KexAlgorithms is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.13	Ensure sshd LoginGraceTime is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.14	Ensure sshd LogLevel is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.15	Ensure sshd MACs are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.16	Ensure sshd MaxAuthTries is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.17	Ensure sshd MaxSessions is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.18	Ensure sshd MaxStartups is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.1.19	Ensure sshd PermitEmptyPasswords is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.20	Ensure sshd PermitRootLogin is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.21	Ensure sshd PermitUserEnvironment is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.22	Ensure sshd UsePAM is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.2</b>	<b>Configure privilege escalation</b>		
5.2.1	Ensure sudo is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure sudo commands use pty (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure sudo log file exists (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure users must provide password for privilege escalation (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure re-authentication for privilege escalation is not disabled globally (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure sudo authentication timeout is configured correctly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure access to the su command is restricted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.3</b>	<b>Pluggable Authentication Modules</b>		
<b>5.3.1</b>	<b>Configure PAM software packages</b>		
5.3.1.1	Ensure latest version of pam is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1.2	Ensure libpam-modules is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1.3	Ensure libpam-pwquality is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.3.2</b>	<b>Configure pam-auth-update profiles</b>		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.3.2.1	Ensure pam_unix module is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.2	Ensure pam_faillock module is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.3	Ensure pam_pwquality module is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.4	Ensure pam_pwhistory module is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.3.3</b>	<b>Configure PAM Arguments</b>		
<b>5.3.3.1</b>	<b>Configure pam_faillock module</b>		
5.3.3.1.1	Ensure password failed attempts lockout is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.2	Ensure password unlock time is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.3	Ensure password failed attempts lockout includes root account (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.3.3.2</b>	<b>Configure pam_pwquality module</b>		
5.3.3.2.1	Ensure password number of changed characters is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.2	Ensure minimum password length is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.3	Ensure password complexity is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.4	Ensure password same consecutive characters is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.5	Ensure password maximum sequential characters is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.6	Ensure password dictionary check is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.7	Ensure password quality checking is enforced (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.3.3.2.8	Ensure password quality is enforced for the root user (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.3.3.3</b>	<b>Configure pam_pwhistory module</b>		
5.3.3.3.1	Ensure password history remember is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.2	Ensure password history is enforced for the root user (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.3	Ensure pam_pwhistory includes use_authok (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.3.3.4</b>	<b>Configure pam_unix module</b>		
5.3.3.4.1	Ensure pam_unix does not include nullok (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.2	Ensure pam_unix does not include remember (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.3	Ensure pam_unix includes a strong password hashing algorithm (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.4	Ensure pam_unix includes use_authok (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.4</b>	<b>User Accounts and Environment</b>		
<b>5.4.1</b>	<b>Configure shadow password suite parameters</b>		
5.4.1.1	Ensure password expiration is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.2	Ensure minimum password age is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.3	Ensure password expiration warning days is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.4	Ensure strong password hashing algorithm is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.5	Ensure inactive password lock is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.4.1.6	Ensure all users last password change date is in the past (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.4.2</b>	<b>Configure root and system accounts and environment</b>		
5.4.2.1	Ensure root is the only UID 0 account (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.2	Ensure root is the only GID 0 account (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.3	Ensure group root is the only GID 0 group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.4	Ensure root password is set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.5	Ensure root path integrity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.6	Ensure root user umask is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.7	Ensure system accounts do not have a valid login shell (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.8	Ensure accounts without a valid login shell are locked (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.4.3</b>	<b>Configure user default environment</b>		
5.4.3.1	Ensure nologin is not listed in /etc/shells (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.2	Ensure default user shell timeout is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.3	Ensure default user umask is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6</b>	<b>Logging and Auditing</b>		
<b>6.1</b>	<b>Configure Integrity Checking</b>		
6.1.1	Ensure AIDE is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure filesystem integrity is regularly checked (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.1.3	Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6.2</b>	<b>System Logging</b>		
<b>6.2.1</b>	<b>Configure journald</b>		
<b>6.2.1.1</b>	<b>Configure systemd-journald service</b>		
6.2.1.1.1	Ensure journald service is enabled and active (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.2	Ensure journald log file access is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.3	Ensure journald log file rotation is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.4	Ensure journald ForwardToSyslog is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.5	Ensure journald Storage is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.6	Ensure journald Compress is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6.2.1.2</b>	<b>Configure systemd-journal-remote</b>		
6.2.1.2.1	Ensure systemd-journal-remote is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.2	Ensure systemd-journal-remote authentication is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.3	Ensure systemd-journal-upload is enabled and active (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.4	Ensure systemd-journal-remote service is not in use (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6.2.2</b>	<b>Configure Logfiles</b>		
6.2.2.1	Ensure access to all logfiles has been configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6.4</b>	<b>System Auditing</b>		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
<b>6.4.1</b>	<b>Configure auditd Service</b>		
6.4.1.1	Ensure auditd packages are installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.2	Ensure auditd service is enabled and active (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.3	Ensure auditing for processes that start prior to auditd is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.4	Ensure audit_backlog_limit is sufficient (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6.4.2</b>	<b>Configure Data Retention</b>		
6.4.2.1	Ensure audit log storage size is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.2	Ensure audit logs are not automatically deleted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.3	Ensure system is disabled when audit logs are full (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.4	Ensure system warns when audit logs are low on space (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6.4.3</b>	<b>Configure auditd Rules</b>		
6.4.3.1	Ensure changes to system administration scope (sudoers) is collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.2	Ensure actions as another user are always logged (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.3	Ensure events that modify the sudo log file are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.4	Ensure events that modify date and time information are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.5	Ensure events that modify the system's network environment are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.4.3.6	Ensure use of privileged commands are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.7	Ensure unsuccessful file access attempts are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.8	Ensure events that modify user/group information are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.9	Ensure discretionary access control permission modification events are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.10	Ensure successful file system mounts are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.11	Ensure session initiation information is collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.12	Ensure login and logout events are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.13	Ensure file deletion events by users are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.14	Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.19	Ensure kernel module loading unloading and modification is collected (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.4.3.20	Ensure the audit configuration is immutable (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.21	Ensure the running and on disk configuration is the same (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6.4.4</b>	<b>Configure auditd File Access</b>		
6.4.4.1	Ensure audit log files mode is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.2	Ensure audit log files owner is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.3	Ensure audit log files group owner is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.4	Ensure the audit log file directory mode is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.5	Ensure audit configuration files mode is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.6	Ensure audit configuration files owner is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.7	Ensure audit configuration files group owner is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.8	Ensure audit tools mode is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.9	Ensure audit tools owner is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.10	Ensure audit tools group owner is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>7</b>	<b>System Maintenance</b>		
<b>7.1</b>	<b>System File Permissions</b>		
7.1.1	Ensure permissions on /etc/passwd are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.2	Ensure permissions on /etc/passwd- are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.1.3	Ensure permissions on /etc/group are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.4	Ensure permissions on /etc/group- are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.5	Ensure permissions on /etc/shadow are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.6	Ensure permissions on /etc/shadow- are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.7	Ensure permissions on /etc/gshadow are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.8	Ensure permissions on /etc/gshadow- are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.9	Ensure permissions on /etc/shells are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.10	Ensure permissions on /etc/security/opasswd are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.11	Ensure world writable files and directories are secured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.12	Ensure no files or directories without an owner and a group exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.13	Ensure SUID and SGID files are reviewed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>7.2</b>	<b>Local User and Group Settings</b>		
7.2.1	Ensure accounts in /etc/passwd use shadowed passwords (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2.2	Ensure /etc/shadow password fields are not empty (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2.3	Ensure all groups in /etc/passwd exist in /etc/group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.2.4	Ensure shadow group is empty (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2.5	Ensure no duplicate UIDs exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2.6	Ensure no duplicate GIDs exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2.7	Ensure no duplicate user names exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2.8	Ensure no duplicate group names exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2.9	Ensure local interactive user home directories are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2.10	Ensure local interactive user dot files access is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.2.1.3	Ensure nosuid option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.4	Ensure noexec option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.2	Ensure nodev option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.4	Ensure noexec option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.1	Ensure separate partition exists for /home	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.2	Ensure nodev option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.3	Ensure nosuid option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.1	Ensure separate partition exists for /var	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.2	Ensure nodev option set on /var partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.3	Ensure nosuid option set on /var partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.1	Ensure separate partition exists for /var/tmp	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.2	Ensure nodev option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.4	Ensure noexec option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.2	Ensure nodev option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.3	Ensure nosuid option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.4	Ensure noexec option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.1	Ensure GPG keys are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.2	Ensure package manager repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2.1	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.1	Ensure AppArmor is installed	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.3.1.2	Ensure AppArmor is enabled in the bootloader configuration	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.3	Ensure all AppArmor Profiles are in enforce or complain mode	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.4	Ensure all AppArmor Profiles are enforcing	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure bootloader password is set	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure access to bootloader config is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure access to /etc/motd is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure access to /etc/issue is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure access to /etc/issue.net is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.4	Ensure GDM screen locks when the user is idle	<input type="checkbox"/>	<input type="checkbox"/>
1.7.5	Ensure GDM screen locks cannot be overridden	<input type="checkbox"/>	<input type="checkbox"/>
1.7.6	Ensure GDM automatic mounting of removable media is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.7.8	Ensure GDM autorun-never is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.7.9	Ensure GDM autorun-never is not overridden	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	Ensure autofs services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.20	Ensure X window server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure NIS Client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.2	Ensure permissions on /etc/crontab are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.3	Ensure permissions on /etc/cron.hourly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.4	Ensure permissions on /etc/cron.daily are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.5	Ensure permissions on /etc/cron.weekly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.6	Ensure permissions on /etc/cron.monthly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.7	Ensure permissions on /etc/cron.d are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.8	Ensure crontab is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2.1	Ensure at is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1	Ensure ufw is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure iptables-persistent is not installed with ufw	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure ufw service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure ufw loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.1.5	Ensure ufw outbound connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure ufw firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure ufw default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1	Ensure nftables is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	Ensure ufw is uninstalled or disabled with nftables	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure iptables are flushed with nftables	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	Ensure a nftables table exists	<input type="checkbox"/>	<input type="checkbox"/>
4.2.5	Ensure nftables base chains exist	<input type="checkbox"/>	<input type="checkbox"/>
4.2.6	Ensure nftables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.7	Ensure nftables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.8	Ensure nftables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.2.9	Ensure nftables service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.2.10	Ensure nftables rules are permanent	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.1	Ensure iptables packages are installed	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.2	Ensure nftables is not installed with iptables	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.3	Ensure ufw is uninstalled or disabled with iptables	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.1	Ensure iptables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.2	Ensure iptables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.3	Ensure iptables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.4	Ensure iptables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.1	Ensure ip6tables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.2	Ensure ip6tables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.3	Ensure ip6tables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.4	Ensure ip6tables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure permissions on SSH private host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on SSH public host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.1.4	Ensure sshd access is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.14	Ensure sshd LogLevel is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.20	Ensure sshd PermitRootLogin is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure sudo is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure users must provide password for privilege escalation	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure re-authentication for privilege escalation is not disabled globally	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure sudo authentication timeout is configured correctly	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure access to the su command is restricted	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.1	Ensure pam_unix module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.2	Ensure root is the only GID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.3	Ensure group root is the only GID 0 group	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.4	Ensure root password is set	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.6	Ensure root user umask is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.7	Ensure system accounts do not have a valid login shell	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.8	Ensure accounts without a valid login shell are locked	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.2	Ensure default user shell timeout is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.3	Ensure default user umask is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.1	Ensure journald service is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.2	Ensure journald log file access is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.3	Ensure journald log file rotation is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.5	Ensure journald Storage is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.6	Ensure journald Compress is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.1	Ensure systemd-journal-remote is installed	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.2	Ensure systemd-journal-remote authentication is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.3	Ensure systemd-journal-upload is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2.1	Ensure access to all logfiles has been configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.1	Ensure auditd packages are installed	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.4.1.2	Ensure auditd service is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.3	Ensure auditing for processes that start prior to auditd is enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.4	Ensure audit_backlog_limit is sufficient	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.4	Ensure system warns when audit logs are low on space	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.6	Ensure use of privileged commands are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.12	Ensure login and logout events are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.13	Ensure file deletion events by users are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.19	Ensure kernel module loading unloading and modification is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.20	Ensure the audit configuration is immutable	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.1	Ensure audit log files mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.2	Ensure audit log files owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.3	Ensure audit log files group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.4	Ensure the audit log file directory mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.5	Ensure audit configuration files mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.6	Ensure audit configuration files owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.7	Ensure audit configuration files group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.8	Ensure audit tools mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.9	Ensure audit tools owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.10	Ensure audit tools group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.1	Ensure permissions on /etc/passwd are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.2	Ensure permissions on /etc/passwd- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	Ensure permissions on /etc/group are configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
7.1.4	Ensure permissions on /etc/group- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.5	Ensure permissions on /etc/shadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.6	Ensure permissions on /etc/shadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.7	Ensure permissions on /etc/gshadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.8	Ensure permissions on /etc/gshadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.9	Ensure permissions on /etc/shells are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.10	Ensure permissions on /etc/security/opasswd are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.11	Ensure world writable files and directories are secured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.12	Ensure no files or directories without an owner and a group exist	<input type="checkbox"/>	<input type="checkbox"/>
7.1.13	Ensure SUID and SGID files are reviewed	<input type="checkbox"/>	<input type="checkbox"/>
7.2.4	Ensure shadow group is empty	<input type="checkbox"/>	<input type="checkbox"/>
7.2.9	Ensure local interactive user home directories are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.2.10	Ensure local interactive user dot files access is configured	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure cramfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure freevxfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure hfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure hfsplus kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.5	Ensure jffs2 kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.6	Ensure squashfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.7	Ensure udf kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.8	Ensure usb-storage kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.1	Ensure /tmp is a separate partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.2	Ensure nodev option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.3	Ensure nosuid option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.4	Ensure noexec option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.1	Ensure /dev/shm is a separate partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.2	Ensure nodev option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.4	Ensure noexec option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.1	Ensure separate partition exists for /home	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.2	Ensure nodev option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.3	Ensure nosuid option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.1	Ensure separate partition exists for /var	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.2	Ensure nodev option set on /var partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.3	Ensure nosuid option set on /var partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.1	Ensure separate partition exists for /var/tmp	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.2	Ensure nodev option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.4	Ensure noexec option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.1	Ensure separate partition exists for /var/log	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.1.2.6.2	Ensure nodev option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.3	Ensure nosuid option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.4	Ensure noexec option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.1	Ensure separate partition exists for /var/log/audit	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.1	Ensure GPG keys are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.2	Ensure package manager repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2.1	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.1	Ensure AppArmor is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.2	Ensure AppArmor is enabled in the bootloader configuration	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.3	Ensure all AppArmor Profiles are in enforce or complain mode	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.4	Ensure all AppArmor Profiles are enforcing	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure bootloader password is set	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure access to bootloader config is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure address space layout randomization is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure ptrace_scope is restricted	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Ensure Automatic Error Reporting is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure access to /etc/motd is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure access to /etc/issue is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure access to /etc/issue.net is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1	Ensure GDM is removed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.4	Ensure GDM screen locks when the user is idle	<input type="checkbox"/>	<input type="checkbox"/>
1.7.5	Ensure GDM screen locks cannot be overridden	<input type="checkbox"/>	<input type="checkbox"/>
1.7.6	Ensure GDM automatic mounting of removable media is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.7.8	Ensure GDM autorun-never is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.7.9	Ensure GDM autorun-never is not overridden	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.7.10	Ensure XDCMP is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	Ensure autofs services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure avahi daemon services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure dhcp server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Ensure dns server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Ensure dnsmasq services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure ftp server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Ensure ldap server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Ensure message access server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Ensure network file system services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.10	Ensure nis server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.11	Ensure print server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure rpcbind services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.13	Ensure rsync services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure samba file server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.15	Ensure snmp services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.16	Ensure tftp server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.17	Ensure web proxy server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.18	Ensure web server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.19	Ensure xinetd services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.20	Ensure X window server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.21	Ensure mail transfer agent is configured for local-only mode	<input type="checkbox"/>	<input type="checkbox"/>
2.1.22	Ensure only approved services are listening on a network interface	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure NIS Client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure rsh client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure talk client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure telnet client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure ldap client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure ftp client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.1	Ensure a single time synchronization daemon is in use	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.2.1	Ensure systemd-timesyncd configured with authorized timeserver	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2	Ensure systemd-timesyncd is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1	Ensure chrony is configured with authorized timeserver	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.2	Ensure chrony is running as user _chrony	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3	Ensure chrony is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.2	Ensure permissions on /etc/crontab are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.3	Ensure permissions on /etc/cron.hourly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.4	Ensure permissions on /etc/cron.daily are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.5	Ensure permissions on /etc/cron.weekly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.6	Ensure permissions on /etc/cron.monthly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.7	Ensure permissions on /etc/cron.d are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.8	Ensure crontab is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2.1	Ensure at is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure IPv6 status is identified	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure bluetooth services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure dccp kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure tipc kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure rds kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure sctp kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure ip forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure bogus icmp responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure broadcast icmp requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure icmp redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure secure icmp redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.3.7	Ensure reverse path filtering is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.8	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.3.10	Ensure tcp syn cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.11	Ensure ipv6 router advertisements are not accepted	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.1.1	Ensure ufw is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure iptables-persistent is not installed with ufw	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure ufw service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure ufw loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure ufw outbound connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure ufw firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure ufw default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1	Ensure nftables is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	Ensure ufw is uninstalled or disabled with nftables	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure iptables are flushed with nftables	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	Ensure a nftables table exists	<input type="checkbox"/>	<input type="checkbox"/>
4.2.5	Ensure nftables base chains exist	<input type="checkbox"/>	<input type="checkbox"/>
4.2.6	Ensure nftables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.7	Ensure nftables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.8	Ensure nftables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.2.9	Ensure nftables service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.2.10	Ensure nftables rules are permanent	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.1	Ensure iptables packages are installed	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.2	Ensure nftables is not installed with iptables	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.3	Ensure ufw is uninstalled or disabled with iptables	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.1	Ensure iptables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.2	Ensure iptables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.3	Ensure iptables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.4	Ensure iptables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.1	Ensure ip6tables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.2	Ensure ip6tables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.3	Ensure ip6tables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.4	Ensure ip6tables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure permissions on SSH private host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on SSH public host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure sshd access is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure sshd Ciphers are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.8	Ensure sshd DisableForwarding is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.9	Ensure sshd GSSAPIAuthentication is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.11	Ensure sshd IgnoreRhosts is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.12	Ensure sshd KexAlgorithms is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.14	Ensure sshd LogLevel is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.15	Ensure sshd MACs are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.19	Ensure sshd PermitEmptyPasswords is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.20	Ensure sshd PermitRootLogin is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.22	Ensure sshd UsePAM is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure sudo is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure sudo log file exists	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure users must provide password for privilege escalation	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure re-authentication for privilege escalation is not disabled globally	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure sudo authentication timeout is configured correctly	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure access to the su command is restricted	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.1	Ensure pam_unix module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.2	Ensure pam_faillock module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.3	Ensure pam_pwquality module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.4	Ensure pam_pwhistory module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.1	Ensure password failed attempts lockout is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.2	Ensure password unlock time is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.3.3.1.3	Ensure password failed attempts lockout includes root account	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.1	Ensure password number of changed characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.2	Ensure minimum password length is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.3	Ensure password complexity is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.4	Ensure password same consecutive characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.5	Ensure password maximum sequential characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.6	Ensure password dictionary check is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.7	Ensure password quality checking is enforced	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.8	Ensure password quality is enforced for the root user	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.1	Ensure password history remember is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.2	Ensure password history is enforced for the root user	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.3	Ensure pam_pwhistory includes use_authok	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.1	Ensure pam_unix does not include nullok	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.2	Ensure pam_unix does not include remember	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.3	Ensure pam_unix includes a strong password hashing algorithm	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.4	Ensure pam_unix includes use_authok	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.1	Ensure password expiration is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.2	Ensure minimum password age is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.3	Ensure password expiration warning days is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.4	Ensure strong password hashing algorithm is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.5	Ensure inactive password lock is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.6	Ensure all users last password change date is in the past	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.2	Ensure root is the only GID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.3	Ensure group root is the only GID 0 group	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.4	Ensure root password is set	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.6	Ensure root user umask is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.7	Ensure system accounts do not have a valid login shell	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.8	Ensure accounts without a valid login shell are locked	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.4.3.2	Ensure default user shell timeout is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.3	Ensure default user umask is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.1	Ensure journald service is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.2	Ensure journald log file access is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.3	Ensure journald log file rotation is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.4	Ensure journald ForwardToSyslog is disabled	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.5	Ensure journald Storage is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.6	Ensure journald Compress is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.1	Ensure systemd-journal-remote is installed	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.2	Ensure systemd-journal-remote authentication is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.3	Ensure systemd-journal-upload is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.4	Ensure systemd-journal-remote service is not in use	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2.1	Ensure access to all logfiles has been configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.1	Ensure auditd packages are installed	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.2	Ensure auditd service is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.3	Ensure auditing for processes that start prior to auditd is enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.4	Ensure audit_backlog_limit is sufficient	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.1	Ensure audit log storage size is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.2	Ensure audit logs are not automatically deleted	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.4	Ensure system warns when audit logs are low on space	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.1	Ensure changes to system administration scope (sudoers) is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.2	Ensure actions as another user are always logged	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.3	Ensure events that modify the sudo log file are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.4	Ensure events that modify date and time information are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.5	Ensure events that modify the system's network environment are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.6	Ensure use of privileged commands are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.8	Ensure events that modify user/group information are collected	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.4.3.9	Ensure discretionary access control permission modification events are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.10	Ensure successful file system mounts are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.11	Ensure session initiation information is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.12	Ensure login and logout events are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.13	Ensure file deletion events by users are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.14	Ensure events that modify the system's Mandatory Access Controls are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.16	Ensure successful and unsuccessful attempts to use the setfacil command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.19	Ensure kernel module loading unloading and modification is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.20	Ensure the audit configuration is immutable	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.21	Ensure the running and on disk configuration is the same	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.1	Ensure audit log files mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.2	Ensure audit log files owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.3	Ensure audit log files group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.4	Ensure the audit log file directory mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.5	Ensure audit configuration files mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.6	Ensure audit configuration files owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.7	Ensure audit configuration files group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.8	Ensure audit tools mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.9	Ensure audit tools owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.10	Ensure audit tools group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.1	Ensure permissions on /etc/passwd are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.2	Ensure permissions on /etc/passwd- are configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
7.1.3	Ensure permissions on /etc/group are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.4	Ensure permissions on /etc/group- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.5	Ensure permissions on /etc/shadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.6	Ensure permissions on /etc/shadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.7	Ensure permissions on /etc/gshadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.8	Ensure permissions on /etc/gshadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.9	Ensure permissions on /etc/shells are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.10	Ensure permissions on /etc/security/opasswd are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.11	Ensure world writable files and directories are secured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.12	Ensure no files or directories without an owner and a group exist	<input type="checkbox"/>	<input type="checkbox"/>
7.1.13	Ensure SUID and SGID files are reviewed	<input type="checkbox"/>	<input type="checkbox"/>
7.2.1	Ensure accounts in /etc/passwd use shadowed passwords	<input type="checkbox"/>	<input type="checkbox"/>
7.2.2	Ensure /etc/shadow password fields are not empty	<input type="checkbox"/>	<input type="checkbox"/>
7.2.4	Ensure shadow group is empty	<input type="checkbox"/>	<input type="checkbox"/>
7.2.9	Ensure local interactive user home directories are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.2.10	Ensure local interactive user dot files access is configured	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure cramfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure freevxfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure hfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure hfsplus kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.5	Ensure jffs2 kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.6	Ensure squashfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.7	Ensure udf kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.8	Ensure usb-storage kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.1	Ensure /tmp is a separate partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.2	Ensure nodev option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.3	Ensure nosuid option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.4	Ensure noexec option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.1	Ensure /dev/shm is a separate partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.2	Ensure nodev option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.4	Ensure noexec option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.1	Ensure separate partition exists for /home	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.2	Ensure nodev option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.3	Ensure nosuid option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.1	Ensure separate partition exists for /var	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.2	Ensure nodev option set on /var partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.3	Ensure nosuid option set on /var partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.1	Ensure separate partition exists for /var/tmp	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.2	Ensure nodev option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.4	Ensure noexec option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.1	Ensure separate partition exists for /var/log	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.1.2.6.2	Ensure nodev option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.3	Ensure nosuid option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.4	Ensure noexec option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.1	Ensure separate partition exists for /var/log/audit	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.1	Ensure GPG keys are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.2	Ensure package manager repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2.1	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.1	Ensure AppArmor is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.2	Ensure AppArmor is enabled in the bootloader configuration	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.3	Ensure all AppArmor Profiles are in enforce or complain mode	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.4	Ensure all AppArmor Profiles are enforcing	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure bootloader password is set	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure access to bootloader config is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure address space layout randomization is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure ptrace_scope is restricted	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Ensure prelink is not installed	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Ensure Automatic Error Reporting is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure access to /etc/motd is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure access to /etc/issue is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure access to /etc/issue.net is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1	Ensure GDM is removed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.4	Ensure GDM screen locks when the user is idle	<input type="checkbox"/>	<input type="checkbox"/>
1.7.5	Ensure GDM screen locks cannot be overridden	<input type="checkbox"/>	<input type="checkbox"/>
1.7.6	Ensure GDM automatic mounting of removable media is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.7.8	Ensure GDM autorun-never is enabled	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.7.9	Ensure GDM autorun-never is not overridden	<input type="checkbox"/>	<input type="checkbox"/>
1.7.10	Ensure XDCMP is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	Ensure autofs services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure avahi daemon services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure dhcp server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Ensure dns server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Ensure dnsmasq services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure ftp server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Ensure ldap server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Ensure message access server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Ensure network file system services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.10	Ensure nis server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.11	Ensure print server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure rpcbind services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.13	Ensure rsync services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure samba file server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.15	Ensure snmp services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.16	Ensure tftp server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.17	Ensure web proxy server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.18	Ensure web server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.19	Ensure xinetd services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.20	Ensure X window server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.21	Ensure mail transfer agent is configured for local-only mode	<input type="checkbox"/>	<input type="checkbox"/>
2.1.22	Ensure only approved services are listening on a network interface	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure NIS Client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure rsh client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure talk client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure telnet client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure ldap client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure ftp client is not installed	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.1	Ensure a single time synchronization daemon is in use	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1	Ensure systemd-timesyncd configured with authorized timeserver	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2	Ensure systemd-timesyncd is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1	Ensure chrony is configured with authorized timeserver	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.2	Ensure chrony is running as user_chrony	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3	Ensure chrony is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.2	Ensure permissions on /etc/crontab are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.3	Ensure permissions on /etc/cron.hourly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.4	Ensure permissions on /etc/cron.daily are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.5	Ensure permissions on /etc/cron.weekly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.6	Ensure permissions on /etc/cron.monthly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.7	Ensure permissions on /etc/cron.d are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.8	Ensure crontab is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2.1	Ensure at is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure IPv6 status is identified	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure wireless interfaces are disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure bluetooth services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure dccp kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure tipc kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure rds kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure sctp kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure ip forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure bogus icmp responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure broadcast icmp requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure icmp redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure secure icmp redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.3.7	Ensure reverse path filtering is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.8	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.3.10	Ensure tcp syn cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.11	Ensure ipv6 router advertisements are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1	Ensure ufw is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure iptables-persistent is not installed with ufw	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure ufw service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure ufw loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure ufw outbound connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure ufw firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure ufw default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1	Ensure nftables is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	Ensure ufw is uninstalled or disabled with nftables	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure iptables are flushed with nftables	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	Ensure a nftables table exists	<input type="checkbox"/>	<input type="checkbox"/>
4.2.5	Ensure nftables base chains exist	<input type="checkbox"/>	<input type="checkbox"/>
4.2.6	Ensure nftables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.7	Ensure nftables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.8	Ensure nftables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.2.9	Ensure nftables service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.2.10	Ensure nftables rules are permanent	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.1	Ensure iptables packages are installed	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.2	Ensure nftables is not installed with iptables	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.3	Ensure ufw is uninstalled or disabled with iptables	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.1	Ensure iptables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.2	Ensure iptables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.3	Ensure iptables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.4	Ensure iptables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.1	Ensure ip6tables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.2	Ensure ip6tables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.3	Ensure ip6tables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.3.3.4	Ensure ip6tables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure permissions on SSH private host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on SSH public host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure sshd access is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure sshd Ciphers are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.8	Ensure sshd DisableForwarding is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.9	Ensure sshd GSSAPIAuthentication is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.11	Ensure sshd IgnoreRhosts is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.12	Ensure sshd KexAlgorithms is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.14	Ensure sshd LogLevel is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.15	Ensure sshd MACs are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.16	Ensure sshd MaxAuthTries is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.19	Ensure sshd PermitEmptyPasswords is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.20	Ensure sshd PermitRootLogin is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.22	Ensure sshd UsePAM is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure sudo is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure sudo log file exists	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure users must provide password for privilege escalation	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure re-authentication for privilege escalation is not disabled globally	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure sudo authentication timeout is configured correctly	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure access to the su command is restricted	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.1	Ensure pam_unix module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.2	Ensure pam_faillock module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.3	Ensure pam_pwquality module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.4	Ensure pam_pwhistory module is enabled	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.3.3.1.1	Ensure password failed attempts lockout is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.2	Ensure password unlock time is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.3	Ensure password failed attempts lockout includes root account	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.1	Ensure password number of changed characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.2	Ensure minimum password length is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.3	Ensure password complexity is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.4	Ensure password same consecutive characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.5	Ensure password maximum sequential characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.6	Ensure password dictionary check is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.7	Ensure password quality checking is enforced	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.8	Ensure password quality is enforced for the root user	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.1	Ensure password history remember is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.2	Ensure password history is enforced for the root user	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.3	Ensure pam_pwhistory includes use_authtok	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.1	Ensure pam_unix does not include nullok	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.2	Ensure pam_unix does not include remember	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.3	Ensure pam_unix includes a strong password hashing algorithm	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.4	Ensure pam_unix includes use_authtok	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.1	Ensure password expiration is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.2	Ensure minimum password age is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.3	Ensure password expiration warning days is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.4	Ensure strong password hashing algorithm is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.5	Ensure inactive password lock is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.6	Ensure all users last password change date is in the past	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.2	Ensure root is the only GID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.3	Ensure group root is the only GID 0 group	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.4	Ensure root password is set	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.6	Ensure root user umask is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.4.2.7	Ensure system accounts do not have a valid login shell	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.8	Ensure accounts without a valid login shell are locked	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.2	Ensure default user shell timeout is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.3	Ensure default user umask is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Ensure AIDE is installed	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure filesystem integrity is regularly checked	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.1	Ensure journald service is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.2	Ensure journald log file access is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.3	Ensure journald log file rotation is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.4	Ensure journald ForwardToSyslog is disabled	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.5	Ensure journald Storage is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.6	Ensure journald Compress is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.1	Ensure systemd-journal-remote is installed	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.2	Ensure systemd-journal-remote authentication is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.3	Ensure systemd-journal-upload is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.4	Ensure systemd-journal-remote service is not in use	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2.1	Ensure access to all logfiles has been configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.1	Ensure auditd packages are installed	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.2	Ensure auditd service is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.3	Ensure auditing for processes that start prior to auditd is enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.4	Ensure audit_backlog_limit is sufficient	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.1	Ensure audit log storage size is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.2	Ensure audit logs are not automatically deleted	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.4	Ensure system warns when audit logs are low on space	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.1	Ensure changes to system administration scope (sudoers) is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.2	Ensure actions as another user are always logged	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.3	Ensure events that modify the sudo log file are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.4	Ensure events that modify date and time information are collected	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.4.3.5	Ensure events that modify the system's network environment are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.6	Ensure use of privileged commands are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.7	Ensure unsuccessful file access attempts are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.8	Ensure events that modify user/group information are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.9	Ensure discretionary access control permission modification events are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.10	Ensure successful file system mounts are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.11	Ensure session initiation information is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.12	Ensure login and logout events are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.13	Ensure file deletion events by users are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.14	Ensure events that modify the system's Mandatory Access Controls are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.19	Ensure kernel module loading unloading and modification is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.20	Ensure the audit configuration is immutable	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.21	Ensure the running and on disk configuration is the same	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.1	Ensure audit log files mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.2	Ensure audit log files owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.3	Ensure audit log files group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.4	Ensure the audit log file directory mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.5	Ensure audit configuration files mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.6	Ensure audit configuration files owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.7	Ensure audit configuration files group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.4.4.8	Ensure audit tools mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.9	Ensure audit tools owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.10	Ensure audit tools group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.1	Ensure permissions on /etc/passwd are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.2	Ensure permissions on /etc/passwd- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	Ensure permissions on /etc/group are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.4	Ensure permissions on /etc/group- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.5	Ensure permissions on /etc/shadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.6	Ensure permissions on /etc/shadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.7	Ensure permissions on /etc/gshadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.8	Ensure permissions on /etc/gshadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.9	Ensure permissions on /etc/shells are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.10	Ensure permissions on /etc/security/opasswd are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.11	Ensure world writable files and directories are secured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.12	Ensure no files or directories without an owner and a group exist	<input type="checkbox"/>	<input type="checkbox"/>
7.1.13	Ensure SUID and SGID files are reviewed	<input type="checkbox"/>	<input type="checkbox"/>
7.2.1	Ensure accounts in /etc/passwd use shadowed passwords	<input type="checkbox"/>	<input type="checkbox"/>
7.2.2	Ensure /etc/shadow password fields are not empty	<input type="checkbox"/>	<input type="checkbox"/>
7.2.4	Ensure shadow group is empty	<input type="checkbox"/>	<input type="checkbox"/>
7.2.9	Ensure local interactive user home directories are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.2.10	Ensure local interactive user dot files access is configured	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.5.3	Ensure core dumps are restricted	<input type="checkbox"/>	<input type="checkbox"/>
1.6.1	Ensure message of the day is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.6.2	Ensure local login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.6.3	Ensure remote login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.7.2	Ensure GDM login banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.3	Ensure GDM disable-user-list option is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.7.7	Ensure GDM disabling automatic mounting of removable media is not overridden	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.1	Ensure cron daemon is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure sshd Banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.10	Ensure sshd HostbasedAuthentication is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.13	Ensure sshd LoginGraceTime is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.17	Ensure sshd MaxSessions is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.18	Ensure sshd MaxStartups is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.21	Ensure sshd PermitUserEnvironment is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1.1	Ensure latest version of pam is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1.2	Ensure libpam-modules is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1.3	Ensure libpam-pwquality is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.1	Ensure root is the only UID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.5	Ensure root path integrity	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.1	Ensure nologin is not listed in /etc/shells	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Ensure cryptographic mechanisms are used to protect the integrity of audit tools	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.3	Ensure system is disabled when audit logs are full	<input type="checkbox"/>	<input type="checkbox"/>
7.2.3	Ensure all groups in /etc/passwd exist in /etc/group	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
7.2.5	Ensure no duplicate UIDs exist	<input type="checkbox"/>	<input type="checkbox"/>
7.2.6	Ensure no duplicate GIDs exist	<input type="checkbox"/>	<input type="checkbox"/>
7.2.7	Ensure no duplicate user names exist	<input type="checkbox"/>	<input type="checkbox"/>
7.2.8	Ensure no duplicate group names exist	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.8	Ensure usb-storage kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.3	Ensure nosuid option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.4	Ensure noexec option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.2	Ensure nodev option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.4	Ensure noexec option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.1	Ensure separate partition exists for /home	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.2	Ensure nodev option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.3	Ensure nosuid option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.1	Ensure separate partition exists for /var	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.2	Ensure nodev option set on /var partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.3	Ensure nosuid option set on /var partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.1	Ensure separate partition exists for /var/tmp	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.2	Ensure nodev option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.4	Ensure noexec option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.1	Ensure separate partition exists for /var/log	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.2	Ensure nodev option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.3	Ensure nosuid option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.4	Ensure noexec option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.1	Ensure separate partition exists for /var/log/audit	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.1	Ensure GPG keys are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.2	Ensure package manager repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.2.2.1	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.1	Ensure AppArmor is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.2	Ensure AppArmor is enabled in the bootloader configuration	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.3	Ensure all AppArmor Profiles are in enforce or complain mode	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.4	Ensure all AppArmor Profiles are enforcing	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure bootloader password is set	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure access to bootloader config is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure access to /etc/motd is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure access to /etc/issue is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure access to /etc/issue.net is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.4	Ensure GDM screen locks when the user is idle	<input type="checkbox"/>	<input type="checkbox"/>
1.7.5	Ensure GDM screen locks cannot be overridden	<input type="checkbox"/>	<input type="checkbox"/>
1.7.6	Ensure GDM automatic mounting of removable media is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.7.8	Ensure GDM autorun-never is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.7.9	Ensure GDM autorun-never is not overridden	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	Ensure autofs services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.2	Ensure permissions on /etc/crontab are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.3	Ensure permissions on /etc/cron.hourly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.4	Ensure permissions on /etc/cron.daily are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.5	Ensure permissions on /etc/cron.weekly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.6	Ensure permissions on /etc/cron.monthly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.7	Ensure permissions on /etc/cron.d are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.8	Ensure crontab is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2.1	Ensure at is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1	Ensure ufw is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure iptables-persistent is not installed with ufw	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure ufw service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure ufw loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.1.5	Ensure ufw outbound connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure ufw firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure ufw default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1	Ensure nftables is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	Ensure ufw is uninstalled or disabled with nftables	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure iptables are flushed with nftables	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	Ensure a nftables table exists	<input type="checkbox"/>	<input type="checkbox"/>
4.2.5	Ensure nftables base chains exist	<input type="checkbox"/>	<input type="checkbox"/>
4.2.6	Ensure nftables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.7	Ensure nftables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.8	Ensure nftables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.2.9	Ensure nftables service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.2.10	Ensure nftables rules are permanent	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.1	Ensure iptables packages are installed	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.2	Ensure nftables is not installed with iptables	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.3	Ensure ufw is uninstalled or disabled with iptables	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.1	Ensure iptables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.2	Ensure iptables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.3	Ensure iptables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.4	Ensure iptables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.1	Ensure ip6tables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.2	Ensure ip6tables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.3	Ensure ip6tables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.4	Ensure ip6tables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure permissions on SSH private host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on SSH public host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.1.4	Ensure sshd access is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.9	Ensure sshd GSSAPIAuthentication is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.11	Ensure sshd IgnoreRhosts is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.14	Ensure sshd LogLevel is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.19	Ensure sshd PermitEmptyPasswords is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.20	Ensure sshd PermitRootLogin is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.22	Ensure sshd UsePAM is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure sudo is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure users must provide password for privilege escalation	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure re-authentication for privilege escalation is not disabled globally	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure sudo authentication timeout is configured correctly	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure access to the su command is restricted	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.1	Ensure pam_unix module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.2	Ensure pam_faillock module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.3	Ensure pam_pwquality module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.4	Ensure pam_pwhistory module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.1	Ensure password failed attempts lockout is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.2	Ensure password unlock time is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.3	Ensure password failed attempts lockout includes root account	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.1	Ensure password number of changed characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.2	Ensure minimum password length is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.3	Ensure password complexity is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.4	Ensure password same consecutive characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.5	Ensure password maximum sequential characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.6	Ensure password dictionary check is enabled	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.3.3.2.7	Ensure password quality checking is enforced	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.8	Ensure password quality is enforced for the root user	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.1	Ensure password history remember is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.2	Ensure password history is enforced for the root user	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.1	Ensure pam_unix does not include nullok	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.2	Ensure pam_unix does not include remember	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.1	Ensure password expiration is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.2	Ensure minimum password age is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.3	Ensure password expiration warning days is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.5	Ensure inactive password lock is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.6	Ensure all users last password change date is in the past	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.2	Ensure root is the only GID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.3	Ensure group root is the only GID 0 group	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.4	Ensure root password is set	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.6	Ensure root user umask is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.7	Ensure system accounts do not have a valid login shell	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.8	Ensure accounts without a valid login shell are locked	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.2	Ensure default user shell timeout is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.3	Ensure default user umask is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.1	Ensure journald service is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.2	Ensure journald log file access is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.3	Ensure journald log file rotation is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.4	Ensure journald ForwardToSyslog is disabled	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.5	Ensure journald Storage is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.6	Ensure journald Compress is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.1	Ensure systemd-journal-remote is installed	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.2	Ensure systemd-journal-remote authentication is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.3	Ensure systemd-journal-upload is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2.1	Ensure access to all logfiles has been configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.2	Ensure auditd service is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.4.1.3	Ensure auditing for processes that start prior to audited is enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.4	Ensure audit_backlog_limit is sufficient	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.1	Ensure audit log storage size is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.2	Ensure audit logs are not automatically deleted	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.3	Ensure system is disabled when audit logs are full	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.4	Ensure system warns when audit logs are low on space	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.16	Ensure successful and unsuccessful attempts to use the setfaci command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.20	Ensure the audit configuration is immutable	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.1	Ensure audit log files mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.2	Ensure audit log files owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.3	Ensure audit log files group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.4	Ensure the audit log file directory mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.5	Ensure audit configuration files mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.6	Ensure audit configuration files owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.7	Ensure audit configuration files group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.8	Ensure audit tools mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.9	Ensure audit tools owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.10	Ensure audit tools group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.1	Ensure permissions on /etc/passwd are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.2	Ensure permissions on /etc/passwd- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	Ensure permissions on /etc/group are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.4	Ensure permissions on /etc/group- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.5	Ensure permissions on /etc/shadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.6	Ensure permissions on /etc/shadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>

<b>Recommendation</b>		<b>Set Correctly</b>	
		<b>Yes</b>	<b>No</b>
7.1.7	Ensure permissions on /etc/gshadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.8	Ensure permissions on /etc/gshadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.9	Ensure permissions on /etc/shells are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.10	Ensure permissions on /etc/security/opasswd are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.11	Ensure world writable files and directories are secured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.12	Ensure no files or directories without an owner and a group exist	<input type="checkbox"/>	<input type="checkbox"/>
7.1.13	Ensure SUID and SGID files are reviewed	<input type="checkbox"/>	<input type="checkbox"/>
7.2.2	Ensure /etc/shadow password fields are not empty	<input type="checkbox"/>	<input type="checkbox"/>
7.2.3	Ensure all groups in /etc/passwd exist in /etc/group	<input type="checkbox"/>	<input type="checkbox"/>
7.2.4	Ensure shadow group is empty	<input type="checkbox"/>	<input type="checkbox"/>
7.2.9	Ensure local interactive user home directories are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.2.10	Ensure local interactive user dot files access is configured	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v8 IG 2 Mapped Recommendations

	Recommendation	Set Correctly	
		Yes	No
1.1.1.1	Ensure cramfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure freevxfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure hfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure hfsplus kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.5	Ensure jffs2 kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.6	Ensure squashfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.7	Ensure udf kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.8	Ensure usb-storage kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.1	Ensure /tmp is a separate partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.2	Ensure nodev option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.3	Ensure nosuid option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.4	Ensure noexec option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.1	Ensure /dev/shm is a separate partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.2	Ensure nodev option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.4	Ensure noexec option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.1	Ensure separate partition exists for /home	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.2	Ensure nodev option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.3	Ensure nosuid option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.1	Ensure separate partition exists for /var	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.2	Ensure nodev option set on /var partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.3	Ensure nosuid option set on /var partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.1	Ensure separate partition exists for /var/tmp	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.2	Ensure nodev option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.4	Ensure noexec option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.1	Ensure separate partition exists for /var/log	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.1.2.6.2	Ensure nodev option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.3	Ensure nosuid option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.4	Ensure noexec option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.1	Ensure separate partition exists for /var/log/audit	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.1	Ensure GPG keys are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.2	Ensure package manager repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2.1	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.1	Ensure AppArmor is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.2	Ensure AppArmor is enabled in the bootloader configuration	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.3	Ensure all AppArmor Profiles are in enforce or complain mode	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.4	Ensure all AppArmor Profiles are enforcing	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure bootloader password is set	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure access to bootloader config is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure address space layout randomization is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure ptrace_scope is restricted	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Ensure Automatic Error Reporting is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure access to /etc/motd is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure access to /etc/issue is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure access to /etc/issue.net is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1	Ensure GDM is removed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.4	Ensure GDM screen locks when the user is idle	<input type="checkbox"/>	<input type="checkbox"/>
1.7.5	Ensure GDM screen locks cannot be overridden	<input type="checkbox"/>	<input type="checkbox"/>
1.7.6	Ensure GDM automatic mounting of removable media is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.7.8	Ensure GDM autorun-never is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.7.9	Ensure GDM autorun-never is not overridden	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.7.10	Ensure XDCMP is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	Ensure autofs services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure avahi daemon services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure dhcp server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Ensure dns server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Ensure dnsmasq services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure ftp server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Ensure ldap server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Ensure message access server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Ensure network file system services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.10	Ensure nis server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.11	Ensure print server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure rpcbind services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.13	Ensure rsync services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure samba file server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.15	Ensure snmp services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.16	Ensure tftp server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.17	Ensure web proxy server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.18	Ensure web server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.19	Ensure xinetd services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.20	Ensure X window server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.21	Ensure mail transfer agent is configured for local-only mode	<input type="checkbox"/>	<input type="checkbox"/>
2.1.22	Ensure only approved services are listening on a network interface	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure NIS Client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure rsh client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure talk client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure telnet client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure ldap client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure ftp client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.1	Ensure a single time synchronization daemon is in use	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.2.1	Ensure systemd-timesyncd configured with authorized timeserver	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2	Ensure systemd-timesyncd is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1	Ensure chrony is configured with authorized timeserver	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.2	Ensure chrony is running as user _chrony	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3	Ensure chrony is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.2	Ensure permissions on /etc/crontab are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.3	Ensure permissions on /etc/cron.hourly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.4	Ensure permissions on /etc/cron.daily are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.5	Ensure permissions on /etc/cron.weekly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.6	Ensure permissions on /etc/cron.monthly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.7	Ensure permissions on /etc/cron.d are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.8	Ensure crontab is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2.1	Ensure at is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure IPv6 status is identified	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure wireless interfaces are disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure bluetooth services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure dccp kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure tipc kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure rds kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure sctp kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure ip forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure bogus icmp responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure broadcast icmp requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure icmp redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure secure icmp redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.3.7	Ensure reverse path filtering is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.8	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.3.10	Ensure tcp syn cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.3.11	Ensure ipv6 router advertisements are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1	Ensure ufw is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure iptables-persistent is not installed with ufw	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure ufw service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure ufw loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure ufw outbound connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure ufw firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure ufw default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1	Ensure nftables is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	Ensure ufw is uninstalled or disabled with nftables	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure iptables are flushed with nftables	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	Ensure a nftables table exists	<input type="checkbox"/>	<input type="checkbox"/>
4.2.5	Ensure nftables base chains exist	<input type="checkbox"/>	<input type="checkbox"/>
4.2.6	Ensure nftables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.7	Ensure nftables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.8	Ensure nftables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.2.9	Ensure nftables service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.2.10	Ensure nftables rules are permanent	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.1	Ensure iptables packages are installed	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.2	Ensure nftables is not installed with iptables	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.3	Ensure ufw is uninstalled or disabled with iptables	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.1	Ensure iptables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.2	Ensure iptables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.3	Ensure iptables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.4	Ensure iptables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.1	Ensure ip6tables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.2	Ensure ip6tables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.3	Ensure ip6tables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.4	Ensure ip6tables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure permissions on SSH private host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on SSH public host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure sshd access is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure sshd Ciphers are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.8	Ensure sshd DisableForwarding is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.9	Ensure sshd GSSAPIAuthentication is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.11	Ensure sshd IgnoreRhosts is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.12	Ensure sshd KexAlgorithms is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.14	Ensure sshd LogLevel is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.15	Ensure sshd MACs are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.16	Ensure sshd MaxAuthTries is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.19	Ensure sshd PermitEmptyPasswords is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.20	Ensure sshd PermitRootLogin is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.22	Ensure sshd UsePAM is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure sudo is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure sudo log file exists	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure users must provide password for privilege escalation	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure re-authentication for privilege escalation is not disabled globally	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure sudo authentication timeout is configured correctly	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure access to the su command is restricted	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.1	Ensure pam_unix module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.2	Ensure pam_faillock module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.3	Ensure pam_pwquality module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.4	Ensure pam_pwhistory module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.1	Ensure password failed attempts lockout is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.3.3.1.2	Ensure password unlock time is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.3	Ensure password failed attempts lockout includes root account	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.1	Ensure password number of changed characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.2	Ensure minimum password length is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.3	Ensure password complexity is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.4	Ensure password same consecutive characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.5	Ensure password maximum sequential characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.6	Ensure password dictionary check is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.7	Ensure password quality checking is enforced	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.8	Ensure password quality is enforced for the root user	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.1	Ensure password history remember is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.2	Ensure password history is enforced for the root user	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.3	Ensure pam_pwhistory includes use_authtok	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.1	Ensure pam_unix does not include nullok	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.2	Ensure pam_unix does not include remember	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.3	Ensure pam_unix includes a strong password hashing algorithm	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.4	Ensure pam_unix includes use_authtok	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.1	Ensure password expiration is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.2	Ensure minimum password age is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.3	Ensure password expiration warning days is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.4	Ensure strong password hashing algorithm is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.5	Ensure inactive password lock is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.6	Ensure all users last password change date is in the past	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.2	Ensure root is the only GID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.3	Ensure group root is the only GID 0 group	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.4	Ensure root password is set	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.6	Ensure root user umask is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.7	Ensure system accounts do not have a valid login shell	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.4.2.8	Ensure accounts without a valid login shell are locked	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.2	Ensure default user shell timeout is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.3	Ensure default user umask is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure filesystem integrity is regularly checked	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.1	Ensure journald service is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.2	Ensure journald log file access is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.3	Ensure journald log file rotation is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.4	Ensure journald ForwardToSyslog is disabled	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.5	Ensure journald Storage is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.6	Ensure journald Compress is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.1	Ensure systemd-journal-remote is installed	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.2	Ensure systemd-journal-remote authentication is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.3	Ensure systemd-journal-upload is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.4	Ensure systemd-journal-remote service is not in use	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2.1	Ensure access to all logfiles has been configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.1	Ensure auditd packages are installed	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.2	Ensure auditd service is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.3	Ensure auditing for processes that start prior to auditd is enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.4	Ensure audit_backlog_limit is sufficient	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.1	Ensure audit log storage size is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.2	Ensure audit logs are not automatically deleted	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.3	Ensure system is disabled when audit logs are full	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.4	Ensure system warns when audit logs are low on space	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.1	Ensure changes to system administration scope (sudoers) is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.2	Ensure actions as another user are always logged	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.3	Ensure events that modify the sudo log file are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.4	Ensure events that modify date and time information are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.5	Ensure events that modify the system's network environment are collected	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.4.3.6	Ensure use of privileged commands are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.7	Ensure unsuccessful file access attempts are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.8	Ensure events that modify user/group information are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.9	Ensure discretionary access control permission modification events are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.10	Ensure successful file system mounts are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.11	Ensure session initiation information is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.12	Ensure login and logout events are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.13	Ensure file deletion events by users are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.14	Ensure events that modify the system's Mandatory Access Controls are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.16	Ensure successful and unsuccessful attempts to use the setfaci command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.19	Ensure kernel module loading unloading and modification is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.20	Ensure the audit configuration is immutable	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.21	Ensure the running and on disk configuration is the same	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.1	Ensure audit log files mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.2	Ensure audit log files owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.3	Ensure audit log files group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.4	Ensure the audit log file directory mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.5	Ensure audit configuration files mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.6	Ensure audit configuration files owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.7	Ensure audit configuration files group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.8	Ensure audit tools mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.9	Ensure audit tools owner is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.4.4.10	Ensure audit tools group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.1	Ensure permissions on /etc/passwd are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.2	Ensure permissions on /etc/passwd- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	Ensure permissions on /etc/group are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.4	Ensure permissions on /etc/group- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.5	Ensure permissions on /etc/shadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.6	Ensure permissions on /etc/shadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.7	Ensure permissions on /etc/gshadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.8	Ensure permissions on /etc/gshadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.9	Ensure permissions on /etc/shells are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.10	Ensure permissions on /etc/security/opasswd are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.11	Ensure world writable files and directories are secured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.12	Ensure no files or directories without an owner and a group exist	<input type="checkbox"/>	<input type="checkbox"/>
7.1.13	Ensure SUID and SGID files are reviewed	<input type="checkbox"/>	<input type="checkbox"/>
7.2.1	Ensure accounts in /etc/passwd use shadowed passwords	<input type="checkbox"/>	<input type="checkbox"/>
7.2.2	Ensure /etc/shadow password fields are not empty	<input type="checkbox"/>	<input type="checkbox"/>
7.2.3	Ensure all groups in /etc/passwd exist in /etc/group	<input type="checkbox"/>	<input type="checkbox"/>
7.2.4	Ensure shadow group is empty	<input type="checkbox"/>	<input type="checkbox"/>
7.2.9	Ensure local interactive user home directories are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.2.10	Ensure local interactive user dot files access is configured	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure cramfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure freevxfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure hfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.4	Ensure hfsplus kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.5	Ensure jffs2 kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.6	Ensure squashfs kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.7	Ensure udf kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.8	Ensure usb-storage kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.1	Ensure /tmp is a separate partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.2	Ensure nodev option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.3	Ensure nosuid option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.1.4	Ensure noexec option set on /tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.1	Ensure /dev/shm is a separate partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.2	Ensure nodev option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2.4	Ensure noexec option set on /dev/shm partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.1	Ensure separate partition exists for /home	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.2	Ensure nodev option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3.3	Ensure nosuid option set on /home partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.1	Ensure separate partition exists for /var	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.2	Ensure nodev option set on /var partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4.3	Ensure nosuid option set on /var partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.1	Ensure separate partition exists for /var/tmp	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.2	Ensure nodev option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.5.4	Ensure noexec option set on /var/tmp partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.1	Ensure separate partition exists for /var/log	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.1.2.6.2	Ensure nodev option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.3	Ensure nosuid option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.6.4	Ensure noexec option set on /var/log partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.1	Ensure separate partition exists for /var/log/audit	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.1	Ensure GPG keys are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1.2	Ensure package manager repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2.1	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.1	Ensure AppArmor is installed	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.2	Ensure AppArmor is enabled in the bootloader configuration	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.3	Ensure all AppArmor Profiles are in enforce or complain mode	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1.4	Ensure all AppArmor Profiles are enforcing	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure bootloader password is set	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure access to bootloader config is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure address space layout randomization is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure ptrace_scope is restricted	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Ensure prelink is not installed	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Ensure Automatic Error Reporting is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Ensure access to /etc/motd is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Ensure access to /etc/issue is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6.6	Ensure access to /etc/issue.net is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.1	Ensure GDM is removed	<input type="checkbox"/>	<input type="checkbox"/>
1.7.4	Ensure GDM screen locks when the user is idle	<input type="checkbox"/>	<input type="checkbox"/>
1.7.5	Ensure GDM screen locks cannot be overridden	<input type="checkbox"/>	<input type="checkbox"/>
1.7.6	Ensure GDM automatic mounting of removable media is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.7.8	Ensure GDM autorun-never is enabled	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
1.7.9	Ensure GDM autorun-never is not overridden	<input type="checkbox"/>	<input type="checkbox"/>
1.7.10	Ensure XDCMP is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	Ensure autofs services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure avahi daemon services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure dhcp server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Ensure dns server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Ensure dnsmasq services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure ftp server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Ensure ldap server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Ensure message access server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Ensure network file system services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.10	Ensure nis server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.11	Ensure print server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure rpcbind services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.13	Ensure rsync services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure samba file server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.15	Ensure snmp services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.16	Ensure tftp server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.17	Ensure web proxy server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.18	Ensure web server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.19	Ensure xinetd services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.20	Ensure X window server services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
2.1.21	Ensure mail transfer agent is configured for local-only mode	<input type="checkbox"/>	<input type="checkbox"/>
2.1.22	Ensure only approved services are listening on a network interface	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure NIS Client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure rsh client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure talk client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure telnet client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure ldap client is not installed	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure ftp client is not installed	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.1.1	Ensure a single time synchronization daemon is in use	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.1	Ensure systemd-timesyncd configured with authorized timeserver	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2	Ensure systemd-timesyncd is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.1	Ensure chrony is configured with authorized timeserver	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.2	Ensure chrony is running as user _chrony	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3.3	Ensure chrony is enabled and running	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.2	Ensure permissions on /etc/crontab are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.3	Ensure permissions on /etc/cron.hourly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.4	Ensure permissions on /etc/cron.daily are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.5	Ensure permissions on /etc/cron.weekly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.6	Ensure permissions on /etc/cron.monthly are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.7	Ensure permissions on /etc/cron.d are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.8	Ensure crontab is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2.1	Ensure at is restricted to authorized users	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure IPv6 status is identified	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure wireless interfaces are disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure bluetooth services are not in use	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure dccp kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure tipc kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure rds kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure sctp kernel module is not available	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure ip forwarding is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Ensure bogus icmp responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Ensure broadcast icmp requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ensure icmp redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.3.6	Ensure secure icmp redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.3.7	Ensure reverse path filtering is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.8	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.3.9	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.3.10	Ensure tcp syn cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.11	Ensure ipv6 router advertisements are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1	Ensure ufw is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure iptables-persistent is not installed with ufw	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure ufw service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure ufw loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure ufw outbound connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure ufw firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
4.1.7	Ensure ufw default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1	Ensure nftables is installed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	Ensure ufw is uninstalled or disabled with nftables	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure iptables are flushed with nftables	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	Ensure a nftables table exists	<input type="checkbox"/>	<input type="checkbox"/>
4.2.5	Ensure nftables base chains exist	<input type="checkbox"/>	<input type="checkbox"/>
4.2.6	Ensure nftables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.7	Ensure nftables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.2.8	Ensure nftables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.2.9	Ensure nftables service is enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.2.10	Ensure nftables rules are permanent	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.1	Ensure iptables packages are installed	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.2	Ensure nftables is not installed with iptables	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1.3	Ensure ufw is uninstalled or disabled with iptables	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.1	Ensure iptables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.2	Ensure iptables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.3	Ensure iptables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2.4	Ensure iptables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.1	Ensure ip6tables default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.2	Ensure ip6tables loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3.3	Ensure ip6tables outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.3.3.4	Ensure ip6tables firewall rules exist for all open ports	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure permissions on SSH private host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure permissions on SSH public host key files are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure sshd access is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure sshd Ciphers are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.8	Ensure sshd DisableForwarding is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.9	Ensure sshd GSSAPIAuthentication is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.11	Ensure sshd IgnoreRhosts is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.12	Ensure sshd KexAlgorithms is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.14	Ensure sshd LogLevel is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.15	Ensure sshd MACs are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.16	Ensure sshd MaxAuthTries is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.19	Ensure sshd PermitEmptyPasswords is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.20	Ensure sshd PermitRootLogin is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.22	Ensure sshd UsePAM is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure sudo is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure sudo log file exists	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure users must provide password for privilege escalation	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure re-authentication for privilege escalation is not disabled globally	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure sudo authentication timeout is configured correctly	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure access to the su command is restricted	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.1	Ensure pam_unix module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.2	Ensure pam_faillock module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.3	Ensure pam_pwquality module is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.4	Ensure pam_pwhistory module is enabled	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.3.3.1.1	Ensure password failed attempts lockout is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.2	Ensure password unlock time is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.1.3	Ensure password failed attempts lockout includes root account	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.1	Ensure password number of changed characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.2	Ensure minimum password length is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.3	Ensure password complexity is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.4	Ensure password same consecutive characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.5	Ensure password maximum sequential characters is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.6	Ensure password dictionary check is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.7	Ensure password quality checking is enforced	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.2.8	Ensure password quality is enforced for the root user	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.1	Ensure password history remember is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.2	Ensure password history is enforced for the root user	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.3.3	Ensure pam_pwhistory includes use_authok	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.1	Ensure pam_unix does not include nullok	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.2	Ensure pam_unix does not include remember	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.3	Ensure pam_unix includes a strong password hashing algorithm	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3.4.4	Ensure pam_unix includes use_authok	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.1	Ensure password expiration is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.2	Ensure minimum password age is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.3	Ensure password expiration warning days is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.4	Ensure strong password hashing algorithm is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.5	Ensure inactive password lock is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1.6	Ensure all users last password change date is in the past	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.2	Ensure root is the only GID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.3	Ensure group root is the only GID 0 group	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.4	Ensure root password is set	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.6	Ensure root user umask is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.4.2.7	Ensure system accounts do not have a valid login shell	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.8	Ensure accounts without a valid login shell are locked	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.2	Ensure default user shell timeout is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.3	Ensure default user umask is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Ensure AIDE is installed	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure filesystem integrity is regularly checked	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.1	Ensure journald service is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.2	Ensure journald log file access is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.3	Ensure journald log file rotation is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.4	Ensure journald ForwardToSyslog is disabled	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.5	Ensure journald Storage is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.1.6	Ensure journald Compress is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.1	Ensure systemd-journal-remote is installed	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.2	Ensure systemd-journal-remote authentication is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.3	Ensure systemd-journal-upload is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1.2.4	Ensure systemd-journal-remote service is not in use	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2.1	Ensure access to all logfiles has been configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.1	Ensure auditd packages are installed	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.2	Ensure auditd service is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.3	Ensure auditing for processes that start prior to auditd is enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.4.1.4	Ensure audit_backlog_limit is sufficient	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.1	Ensure audit log storage size is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.2	Ensure audit logs are not automatically deleted	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.3	Ensure system is disabled when audit logs are full	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2.4	Ensure system warns when audit logs are low on space	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.1	Ensure changes to system administration scope (sudoers) is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.2	Ensure actions as another user are always logged	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.3	Ensure events that modify the sudo log file are collected	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.4.3.4	Ensure events that modify date and time information are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.5	Ensure events that modify the system's network environment are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.6	Ensure use of privileged commands are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.7	Ensure unsuccessful file access attempts are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.8	Ensure events that modify user/group information are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.9	Ensure discretionary access control permission modification events are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.10	Ensure successful file system mounts are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.11	Ensure session initiation information is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.12	Ensure login and logout events are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.13	Ensure file deletion events by users are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.14	Ensure events that modify the system's Mandatory Access Controls are collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.19	Ensure kernel module loading unloading and modification is collected	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.20	Ensure the audit configuration is immutable	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.21	Ensure the running and on disk configuration is the same	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.1	Ensure audit log files mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.2	Ensure audit log files owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.3	Ensure audit log files group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.4	Ensure the audit log file directory mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.5	Ensure audit configuration files mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.6	Ensure audit configuration files owner is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.4.4.7	Ensure audit configuration files group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.8	Ensure audit tools mode is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.9	Ensure audit tools owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4.10	Ensure audit tools group owner is configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.1	Ensure permissions on /etc/passwd are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.2	Ensure permissions on /etc/passwd- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	Ensure permissions on /etc/group are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.4	Ensure permissions on /etc/group- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.5	Ensure permissions on /etc/shadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.6	Ensure permissions on /etc/shadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.7	Ensure permissions on /etc/gshadow are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.8	Ensure permissions on /etc/gshadow- are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.9	Ensure permissions on /etc/shells are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.10	Ensure permissions on /etc/security/opasswd are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.11	Ensure world writable files and directories are secured	<input type="checkbox"/>	<input type="checkbox"/>
7.1.12	Ensure no files or directories without an owner and a group exist	<input type="checkbox"/>	<input type="checkbox"/>
7.1.13	Ensure SUID and SGID files are reviewed	<input type="checkbox"/>	<input type="checkbox"/>
7.2.1	Ensure accounts in /etc/passwd use shadowed passwords	<input type="checkbox"/>	<input type="checkbox"/>
7.2.2	Ensure /etc/shadow password fields are not empty	<input type="checkbox"/>	<input type="checkbox"/>
7.2.3	Ensure all groups in /etc/passwd exist in /etc/group	<input type="checkbox"/>	<input type="checkbox"/>
7.2.4	Ensure shadow group is empty	<input type="checkbox"/>	<input type="checkbox"/>
7.2.9	Ensure local interactive user home directories are configured	<input type="checkbox"/>	<input type="checkbox"/>
7.2.10	Ensure local interactive user dot files access is configured	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.5.3	Ensure core dumps are restricted	<input type="checkbox"/>	<input type="checkbox"/>
1.6.1	Ensure message of the day is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.6.2	Ensure local login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.6.3	Ensure remote login warning banner is configured properly	<input type="checkbox"/>	<input type="checkbox"/>
1.7.2	Ensure GDM login banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7.3	Ensure GDM disable-user-list option is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.7.7	Ensure GDM disabling automatic mounting of removable media is not overridden	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1.1	Ensure cron daemon is enabled and active	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure sshd Banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.10	Ensure sshd HostbasedAuthentication is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.13	Ensure sshd LoginGraceTime is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.17	Ensure sshd MaxSessions is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.18	Ensure sshd MaxStartups is configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.21	Ensure sshd PermitUserEnvironment is disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1.1	Ensure latest version of pam is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1.2	Ensure libpam-modules is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1.3	Ensure libpam-pwquality is installed	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.1	Ensure root is the only UID 0 account	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2.5	Ensure root path integrity	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3.1	Ensure nologin is not listed in /etc/shells	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Ensure cryptographic mechanisms are used to protect the integrity of audit tools	<input type="checkbox"/>	<input type="checkbox"/>
7.2.5	Ensure no duplicate UIDs exist	<input type="checkbox"/>	<input type="checkbox"/>
7.2.6	Ensure no duplicate GIDs exist	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
7.2.7	Ensure no duplicate user names exist	<input type="checkbox"/>	<input type="checkbox"/>
7.2.8	Ensure no duplicate group names exist	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: Change History

Date	Version	Changes for this version
ADDED ITEMS:		
3/29/2024	2.0.0	ADDED SECTION: 1.1 - Filesystem
3/29/2024	2.0.0	ADDED SECTION: 1.1.1 - Configure Filesystem Kernel Modules
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.1.1.1 - Ensure cramfs kernel module is not available
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.1.1.2 - Ensure freevxf kernel module is not available
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.1.1.3 - Ensure hfs kernel module is not available
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.1.1.4 - Ensure hfsplus kernel module is not available
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.1.1.5 - Ensure jffs2 kernel module is not available
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.1.1.6 - Ensure squashfs kernel module is not available
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.1.1.7 - Ensure udf kernel module is not available
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.1.1.8 - Ensure usb-storage kernel module is not available
3/29/2024	2.0.0	ADDED SECTION: 1.1.2 - Configure Filesystem Partitions
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.1.2.2.1 - Ensure /dev/shm is a separate partition
3/29/2024	2.0.0	ADDED SECTION: 1.2 - Package Management
3/29/2024	2.0.0	ADDED SECTION: 1.2.1 - Configure Package Repositories
3/29/2024	2.0.0	ADDED SECTION: 1.2.2 - Configure Package Updates

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	ADDED SECTION: 1.4 - Configure Bootloader
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.4.2 - Ensure access to bootloader config is configured
3/29/2024	2.0.0	ADDED SECTION: 1.5 - Configure Additional Process Hardening
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.5.1 - Ensure address space layout randomization is enabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.5.2 - Ensure ptrace_scope is restricted
3/29/2024	2.0.0	ADDED SECTION: 1.6 - Configure Command Line Warning Banners
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.6.4 - Ensure access to /etc/motd is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.6.5 - Ensure access to /etc/issue is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.6.6 - Ensure access to /etc/issue.net is configured
3/29/2024	2.0.0	ADDED SECTION: 1.7 - Configure GNOME Display Manager
3/29/2024	2.0.0	ADDED RECOMMENDATION: 1.7.1 - Ensure GDM is removed
3/29/2024	2.0.0	ADDED SECTION: 2.1 - Configure Server Services
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.1 - Ensure autofs services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.2 - Ensure avahi daemon services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.3 - Ensure dhcp server services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.4 - Ensure dns server services are not in use

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.5 - Ensure dnsmasq services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.6 - Ensure ftp server services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.7 - Ensure ldap server services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.8 - Ensure message access server services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.9 - Ensure network file system services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.10 - Ensure nis server services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.11 - Ensure print server services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.12 - Ensure rpcbind services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.13 - Ensure rsync services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.14 - Ensure samba file server services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.15 - Ensure snmp services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.16 - Ensure tftp server services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.17 - Ensure web proxy server services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.18 - Ensure web server services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.19 - Ensure xinetd services are not in use

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.20 - Ensure X window server services are not in use
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.1.22 - Ensure only approved services are listening on a network interface
3/29/2024	2.0.0	ADDED SECTION: 2.2 - Configure Client Services
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.2.5 - Ensure ldap client is not installed
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.2.6 - Ensure ftp client is not installed
3/29/2024	2.0.0	ADDED SECTION: 2.4 - Job Schedulers
3/29/2024	2.0.0	ADDED SECTION: 2.4.1 - Configure cron
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.4.1.1 - Ensure cron daemon is enabled and active
3/29/2024	2.0.0	ADDED RECOMMENDATION: 2.4.1.8 - Ensure crontab is restricted to authorized users
3/29/2024	2.0.0	ADDED SECTION: 2.4.2 - Configure at
3/29/2024	2.0.0	ADDED SECTION: 3 - Network
3/29/2024	2.0.0	ADDED SECTION: 3.1 - Configure Network Devices
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.1.1 - Ensure IPv6 status is identified
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.1.3 - Ensure bluetooth services are not in use
3/29/2024	2.0.0	ADDED SECTION: 3.2 - Configure Network Kernel Modules
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.2.1 - Ensure dccp kernel module is not available
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.2.2 - Ensure tipc kernel module is not available

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.2.3 - Ensure rds kernel module is not available
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.2.4 - Ensure sctp kernel module is not available
3/29/2024	2.0.0	ADDED SECTION: 3.3 - Configure Network Kernel Parameters
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.3.1 - Ensure ip forwarding is disabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.3.3 - Ensure bogus icmp responses are ignored
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.3.4 - Ensure broadcast icmp requests are ignored
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.3.5 - Ensure icmp redirects are not accepted
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.3.6 - Ensure secure icmp redirects are not accepted
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.3.7 - Ensure reverse path filtering is enabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.3.10 - Ensure tcp syn cookies is enabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 3.3.11 - Ensure ipv6 router advertisements are not accepted
3/29/2024	2.0.0	ADDED SECTION: 4 - Host Based Firewall
3/29/2024	2.0.0	ADDED SECTION: 5 - Access Control
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.4 - Ensure sshd access is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.5 - Ensure sshd Banner is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.6 - Ensure sshd Ciphers are configured

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.7 - Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.8 - Ensure sshd DisableForwarding is enabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.9 - Ensure sshd GSSAPIAuthentication is disabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.10 - Ensure sshd HostbasedAuthentication is disabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.11 - Ensure sshd IgnoreRhosts is enabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.12 - Ensure sshd KexAlgorithms is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.13 - Ensure sshd LoginGraceTime is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.14 - Ensure sshd LogLevel is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.15 - Ensure sshd MACs are configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.16 - Ensure sshd MaxAuthTries is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.17 - Ensure sshd MaxSessions is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.18 - Ensure sshd MaxStartups is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.19 - Ensure sshd PermitEmptyPasswords is disabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.20 - Ensure sshd PermitRootLogin is disabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.21 - Ensure sshd PermitUserEnvironment is disabled

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.1.22 - Ensure sshd UsePAM is enabled
3/29/2024	2.0.0	ADDED SECTION: 5.3 - Pluggable Authentication Modules
3/29/2024	2.0.0	ADDED SECTION: 5.3.1 - Configure PAM software packages
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.1.1 - Ensure latest version of pam is installed
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.1.2 - Ensure libpam-modules is installed
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.1.3 - Ensure libpam-pwquality is installed
3/29/2024	2.0.0	ADDED SECTION: 5.3.2 - Configure pam-auth-update profiles
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.2.1 - Ensure pam_unix module is enabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.2.2 - Ensure pam_faillock module is enabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.2.3 - Ensure pam_pwquality module is enabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.2.4 - Ensure pam_pwhistory module is enabled
3/29/2024	2.0.0	ADDED SECTION: 5.3.3 - Configure PAM Arguments
3/29/2024	2.0.0	ADDED SECTION: 5.3.3.1 - Configure pam_faillock module
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.1.1 - Ensure password failed attempts lockout is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.1.2 - Ensure password unlock time is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.1.3 - Ensure password failed attempts lockout includes root account
3/29/2024	2.0.0	ADDED SECTION: 5.3.3.2 - Configure pam_pwquality module

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.2.1 - Ensure password number of changed characters is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.2.2 - Ensure minimum password length is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.2.3 - Ensure password complexity is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.2.4 - Ensure password same consecutive characters is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.2.5 - Ensure password maximum sequential characters is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.2.6 - Ensure password dictionary check is enabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.2.7 - Ensure password quality checking is enforced
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.2.8 - Ensure password quality is enforced for the root user
3/29/2024	2.0.0	ADDED SECTION: 5.3.3.3 - Configure pam_pwhistory module
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.3.1 - Ensure password history remember is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.3.2 - Ensure password history is enforced for the root user
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.3.3 - Ensure pam_pwhistory includes use_authok
3/29/2024	2.0.0	ADDED SECTION: 5.3.3.4 - Configure pam_unix module
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.4.1 - Ensure pam_unix does not include nullok
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.4.2 - Ensure pam_unix does not include remember
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.4.3 - Ensure pam_unix includes a strong password hashing algorithm

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.3.3.4.4 - Ensure pam_unix includes use_authok
3/29/2024	2.0.0	ADDED SECTION: 5.4.1 - Configure shadow password suite parameters
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.1.1 - Ensure password expiration is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.1.2 - Ensure minimum password age is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.1.3 - Ensure password expiration warning days is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.1.4 - Ensure strong password hashing algorithm is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.1.5 - Ensure inactive password lock is configured
3/29/2024	2.0.0	ADDED SECTION: 5.4.2 - Configure root and system accounts and environment
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.2.2 - Ensure root is the only GID 0 account
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.2.3 - Ensure group root is the only GID 0 group
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.2.4 - Ensure root password is set
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.2.5 - Ensure root path integrity
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.2.6 - Ensure root user umask is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.2.7 - Ensure system accounts do not have a valid login shell
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.2.8 - Ensure accounts without a valid login shell are locked

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	ADDED SECTION: 5.4.3 - Configure user default environment
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.3.1 - Ensure nologin is not listed in /etc/shells
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.3.2 - Ensure default user shell timeout is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 5.4.3.3 - Ensure default user umask is configured
3/29/2024	2.0.0	ADDED SECTION: 6.1 - Configure Integrity Checking
3/29/2024	2.0.0	ADDED SECTION: 6.2 - System Logging
3/29/2024	2.0.0	ADDED SECTION: 6.2.1.1 - Configure systemd-journald service
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.2.1.1.1 - Ensure journald service is enabled and active
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.2.1.1.2 - Ensure journald log file access is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.2.1.1.3 - Ensure journald log file rotation is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.2.1.1.4 - Ensure journald ForwardToSyslog is disabled
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.2.1.1.5 - Ensure journald Storage is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.2.1.1.6 - Ensure journald Compress is configured
3/29/2024	2.0.0	ADDED SECTION: 6.2.1.2 - Configure systemd-journal-remote
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.2.1.2.2 - Ensure systemd-journal-remote authentication is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.2.1.2.3 - Ensure systemd-journal-upload is enabled and active

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.2.1.2.4 - Ensure systemd-journal-remote service is not in use
3/29/2024	2.0.0	ADDED SECTION: 6.2.2 - Configure Logfiles
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.2.2.1 - Ensure access to all logfiles has been configured
3/29/2024	2.0.0	ADDED SECTION: 6.4 - System Auditing
3/29/2024	2.0.0	ADDED SECTION: 6.4.1 - Configure auditd Service
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.4.1.1 - Ensure auditd packages are installed
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.4.2.4 - Ensure system warns when audit logs are low on space
3/29/2024	2.0.0	ADDED SECTION: 6.4.3 - Configure auditd Rules
3/29/2024	2.0.0	ADDED SECTION: 6.4.4 - Configure auditd File Access
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.4.4.1 - Ensure audit log files mode is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.4.4.2 - Ensure audit log files owner is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.4.4.3 - Ensure audit log files group owner is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.4.4.4 - Ensure the audit log file directory mode is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.4.4.5 - Ensure audit configuration files mode is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.4.4.6 - Ensure audit configuration files owner is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.4.4.7 - Ensure audit configuration files group owner is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.4.4.8 - Ensure audit tools mode is configured

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.4.4.9 - Ensure audit tools owner is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 6.4.4.10 - Ensure audit tools group owner is configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 7.1.9 - Ensure permissions on /etc/shells are configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 7.1.10 - Ensure permissions on /etc/security/opasswd are configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 7.1.11 - Ensure world writable files and directories are secured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 7.1.12 - Ensure no files or directories without an owner and a group exist
3/29/2024	2.0.0	ADDED RECOMMENDATION: 7.1.13 - Ensure SUID and SGID files are reviewed
3/29/2024	2.0.0	ADDED RECOMMENDATION: 7.2.9 - Ensure local interactive user home directories are configured
3/29/2024	2.0.0	ADDED RECOMMENDATION: 7.2.10 - Ensure local interactive user dot files access is configured
<b>DROPPED ITEMS:</b>		
3/29/2024	2.0.0	DROPPED SECTION: 1.1 - Filesystem Configuration
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 1.1.9 - Disable Automounting
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 1.1.10 - Disable USB Storage
3/29/2024	2.0.0	DROPPED SECTION: 1.1.1 - Disable unused filesystems
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 1.1.1.1 - Ensure mounting of cramfs filesystems is disabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 1.1.1.2 - Ensure mounting of squashfs filesystems is disabled

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 1.1.1.3 - Ensure mounting of udf filesystems is disabled
3/29/2024	2.0.0	DROPPED SECTION: 1.2 - Configure Software Updates
3/29/2024	2.0.0	DROPPED SECTION: 1.3 - Filesystem Integrity Checking
3/29/2024	2.0.0	DROPPED SECTION: 1.4 - Secure Boot Settings
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 1.4.2 - Ensure permissions on bootloader config are configured
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 1.4.3 - Ensure authentication required for single user mode
3/29/2024	2.0.0	DROPPED SECTION: 1.5 - Additional Process Hardening
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 1.5.1 - Ensure address space layout randomization (ASLR) is enabled
3/29/2024	2.0.0	DROPPED SECTION: 1.7 - Command Line Warning Banners
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 1.7.4 - Ensure permissions on /etc/motd are configured
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 1.7.5 - Ensure permissions on /etc/issue are configured
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 1.7.6 - Ensure permissions on /etc/issue.net are configured
3/29/2024	2.0.0	DROPPED SECTION: 1.8 - GNOME Display Manager
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 1.8.1 - Ensure GNOME Display Manager is removed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.4 - Ensure nonessential services are removed or masked
3/29/2024	2.0.0	DROPPED SECTION: 2.1.4 - Configure ntp
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.1.4.1 - Ensure ntp access control is configured

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.1.4.2 - Ensure ntp is configured with authorized timeserver
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.1.4.3 - Ensure ntp is running as user ntp
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.1.4.4 - Ensure ntp is enabled and running
3/29/2024	2.0.0	DROPPED SECTION: 2.2 - Special Purpose Services
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.1 - Ensure X Window System is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.2 - Ensure Avahi Server is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.3 - Ensure CUPS is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.4 - Ensure DHCP Server is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.5 - Ensure LDAP server is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.6 - Ensure NFS is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.7 - Ensure DNS Server is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.8 - Ensure FTP Server is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.9 - Ensure HTTP server is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.10 - Ensure IMAP and POP3 server are not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.11 - Ensure Samba is not installed

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.12 - Ensure HTTP Proxy Server is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.13 - Ensure SNMP Server is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.14 - Ensure NIS Server is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.2.16 - Ensure rsync service is either not installed or masked
3/29/2024	2.0.0	DROPPED SECTION: 2.3 - Service Clients
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.3.5 - Ensure LDAP client is not installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 2.3.6 - Ensure RPC is not installed
3/29/2024	2.0.0	DROPPED SECTION: 3 - Network Configuration
3/29/2024	2.0.0	DROPPED SECTION: 3.1 - Disable unused network protocols and devices
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.1.1 - Ensure system is checked to determine if IPv6 is enabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.1.3 - Ensure DCCP is disabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.1.4 - Ensure SCTP is disabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.1.5 - Ensure RDS is disabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.1.6 - Ensure TIPC is disabled
3/29/2024	2.0.0	DROPPED SECTION: 3.2 - Network Parameters (Host Only)
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.2.2 - Ensure IP forwarding is disabled

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	DROPPED SECTION: 3.3 - Network Parameters (Host and Router)
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.3.2 - Ensure ICMP redirects are not accepted
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.3.3 - Ensure secure ICMP redirects are not accepted
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.3.5 - Ensure broadcast ICMP requests are ignored
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.3.6 - Ensure bogus ICMP responses are ignored
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.3.7 - Ensure Reverse Path Filtering is enabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.3.8 - Ensure TCP SYN Cookies is enabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 3.3.9 - Ensure IPv6 router advertisements are not accepted
3/29/2024	2.0.0	DROPPED SECTION: 3.5 - Firewall Configuration
3/29/2024	2.0.0	DROPPED SECTION: 4.1 - Configure System Accounting (auditd)
3/29/2024	2.0.0	DROPPED SECTION: 4.1.1 - Ensure auditing is enabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.1.1.1 - Ensure auditd is installed
3/29/2024	2.0.0	DROPPED SECTION: 4.1.3 - Configure auditd rules
3/29/2024	2.0.0	DROPPED SECTION: 4.1.4 - Configure auditd file access
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.1.4.1 - Ensure audit log files are mode 0640 or less permissive
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.1.4.2 - Ensure only authorized users own audit log files

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.1.4.3 - Ensure only authorized groups are assigned ownership of audit log files
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.1.4.4 - Ensure the audit log directory is 0750 or more restrictive
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.1.4.5 - Ensure audit configuration files are 640 or more restrictive
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.1.4.6 - Ensure audit configuration files are owned by root
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.1.4.7 - Ensure audit configuration files belong to group root
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.1.4.8 - Ensure audit tools are 755 or more restrictive
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.1.4.9 - Ensure audit tools are owned by root
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.1.4.10 - Ensure audit tools belong to group root
3/29/2024	2.0.0	DROPPED SECTION: 4.2 - Configure Logging
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.3 - Ensure all logfiles have appropriate permissions and ownership
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.1.2 - Ensure journald service is enabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.1.3 - Ensure journald is configured to compress large log files
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.1.4 - Ensure journald is configured to write logfiles to persistent disk
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.1.5 - Ensure journald is not configured to send logs to rsyslog
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.1.6 - Ensure journald log rotation is configured per site policy

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.1.7 - Ensure journald default file permissions configured
3/29/2024	2.0.0	DROPPED SECTION: 4.2.1.1 - Ensure journald is configured to send logs to a remote log host
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.1.1.2 - Ensure systemd-journal-remote is configured
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.1.1.3 - Ensure systemd-journal-remote is enabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.1.1.4 - Ensure journald is not configured to receive logs from a remote client
3/29/2024	2.0.0	DROPPED SECTION: 4.2.2 - Configure rsyslog
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.2.1 - Ensure rsyslog is installed
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.2.2 - Ensure rsyslog service is enabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.2.3 - Ensure journald is configured to send logs to rsyslog
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.2.4 - Ensure rsyslog default file permissions are configured
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.2.5 - Ensure logging is configured
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.2.6 - Ensure rsyslog is configured to send logs to a remote log host
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 4.2.2.7 - Ensure rsyslog is not configured to receive logs from a remote client
3/29/2024	2.0.0	DROPPED SECTION: 5 - Access, Authentication and Authorization
3/29/2024	2.0.0	DROPPED SECTION: 5.1 - Configure time-based job schedulers

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.1.1 - Ensure cron daemon is enabled and running
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.1.8 - Ensure cron is restricted to authorized users
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.4 - Ensure SSH access is limited
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.5 - Ensure SSH LogLevel is appropriate
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.6 - Ensure SSH PAM is enabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.7 - Ensure SSH root login is disabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.8 - Ensure SSH HostbasedAuthentication is disabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.9 - Ensure SSH PermitEmptyPasswords is disabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.10 - Ensure SSH PermitUserEnvironment is disabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.11 - Ensure SSH IgnoreRhosts is enabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.12 - Ensure SSH X11 forwarding is disabled
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.13 - Ensure only strong Ciphers are used
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.14 - Ensure only strong MAC algorithms are used
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.15 - Ensure only strong Key Exchange algorithms are used
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.16 - Ensure SSH AllowTcpForwarding is disabled

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.17 - Ensure SSH warning banner is configured
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.18 - Ensure SSH MaxAuthTries is set to 4 or less
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.19 - Ensure SSH MaxStartups is configured
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.20 - Ensure SSH MaxSessions is set to 10 or less
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.21 - Ensure SSH LoginGraceTime is set to one minute or less
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.2.22 - Ensure SSH Idle Timeout Interval is configured
3/29/2024	2.0.0	DROPPED SECTION: 5.4 - Configure PAM
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.4.1 - Ensure password creation requirements are configured
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.4.2 - Ensure lockout for failed password attempts is configured
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.4.3 - Ensure password reuse is limited
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.4.4 - Ensure password hashing algorithm is up to date with the latest standards
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.4.5 - Ensure all current passwords uses the configured hashing algorithm
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.5.2 - Ensure system accounts are secured
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.5.3 - Ensure default group for the root account is GID 0
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.5.4 - Ensure default user umask is 027 or more restrictive

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.5.5 - Ensure default user shell timeout is 900 seconds or less
3/29/2024	2.0.0	DROPPED SECTION: 5.5.1 - Set Shadow Password Suite Parameters
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.5.1.1 - Ensure minimum days between password changes is configured
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.5.1.2 - Ensure password expiration is 365 days or less
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.5.1.3 - Ensure password expiration warning days is 7 or more
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 5.5.1.4 - Ensure inactive password lock is 30 days or less
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.1.9 - Ensure no world writable files exist
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.1.10 - Ensure no unowned files or directories exist
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.1.11 - Ensure no ungrouped files or directories exist
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.1.12 - Audit SUID executables
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.1.13 - Audit SGID executables
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.2.9 - Ensure root PATH Integrity
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.2.11 - Ensure local interactive user home directories exist
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.2.12 - Ensure local interactive users own their home directories
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.2.13 - Ensure local interactive user home directories are mode 750 or more restrictive

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.2.14 - Ensure no local interactive user has .netrc files
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.2.15 - Ensure no local interactive user has .forward files
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.2.16 - Ensure no local interactive user has .rhosts files
3/29/2024	2.0.0	DROPPED RECOMMENDATION: 6.2.17 - Ensure local interactive user dot files are not group or world writable
<b>MOVED ITEMS:</b>		
3/29/2024	2.0.0	MOVED SECTION: 1.1.2.1 - Configure /tmp moved from 1.1.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.1.1 - Ensure /tmp is a separate partition moved from 1.1.2.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.1.2 - Ensure nodev option set on /tmp partition moved from 1.1.2.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.1.3 - Ensure nosuid option set on /tmp partition moved from 1.1.2.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.1.4 - Ensure noexec option set on /tmp partition moved from 1.1.2.3 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 1.1.2.2 - Configure /dev/shm moved from 1.1.8 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.2.2 - Ensure nodev option set on /dev/shm partition moved from 1.1.8.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.2.3 - Ensure nosuid option set on /dev/shm partition moved from 1.1.8.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.2.4 - Ensure noexec option set on /dev/shm partition moved from 1.1.8.2 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 1.1.2.3 - Configure /home moved from 1.1.7 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.3.1 - Ensure separate partition exists for /home moved from 1.1.7.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.3.2 - Ensure nodev option set on /home partition moved from 1.1.7.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.3.3 - Ensure nosuid option set on /home partition moved from 1.1.7.3 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 1.1.2.4 - Configure /var moved from 1.1.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.4.1 - Ensure separate partition exists for /var moved from 1.1.3.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.4.2 - Ensure nodev option set on /var partition moved from 1.1.3.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.4.3 - Ensure nosuid option set on /var partition moved from 1.1.3.3 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 1.1.2.5 - Configure /var/tmp moved from 1.1.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.5.1 - Ensure separate partition exists for /var/tmp moved from 1.1.4.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.5.2 - Ensure nodev option set on /var/tmp partition moved from 1.1.4.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.5.3 - Ensure nosuid option set on /var/tmp partition moved from 1.1.4.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.5.4 - Ensure noexec option set on /var/tmp partition moved from 1.1.4.2 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 1.1.2.6 - Configure /var/log moved from 1.1.5 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.6.1 - Ensure separate partition exists for /var/log moved from 1.1.5.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.6.2 - Ensure nodev option set on /var/log partition moved from 1.1.5.2 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.6.3 - Ensure nosuid option set on /var/log partition moved from 1.1.5.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.6.4 - Ensure noexec option set on /var/log partition moved from 1.1.5.3 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 1.1.2.7 - Configure /var/log/audit moved from 1.1.6 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.7.1 - Ensure separate partition exists for /var/log/audit moved from 1.1.6.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.7.2 - Ensure nodev option set on /var/log/audit partition moved from 1.1.6.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.7.3 - Ensure nosuid option set on /var/log/audit partition moved from 1.1.6.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.1.2.7.4 - Ensure noexec option set on /var/log/audit partition moved from 1.1.6.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.2.1.1 - Ensure GPG keys are configured moved from 1.2.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.2.1.2 - Ensure package manager repositories are configured moved from 1.2.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.2.2.1 - Ensure updates, patches, and additional security software are installed moved from 1.9 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 1.3 - Mandatory Access Control moved from 1.6 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 1.3.1 - Configure AppArmor moved from 1.6.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.3.1.1 - Ensure AppArmor is installed moved from 1.6.1.1 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.3.1.2 - Ensure AppArmor is enabled in the bootloader configuration moved from 1.6.1.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.3.1.3 - Ensure all AppArmor Profiles are in enforce or complain mode moved from 1.6.1.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.3.1.4 - Ensure all AppArmor Profiles are enforcing moved from 1.6.1.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.5.3 - Ensure core dumps are restricted moved from 1.5.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.5.4 - Ensure prelink is not installed moved from 1.5.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.5.5 - Ensure Automatic Error Reporting is not enabled moved from 1.5.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.6.1 - Ensure message of the day is configured properly moved from 1.7.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.6.2 - Ensure local login warning banner is configured properly moved from 1.7.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.6.3 - Ensure remote login warning banner is configured properly moved from 1.7.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.7.2 - Ensure GDM login banner is configured moved from 1.8.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.7.3 - Ensure GDM disable-user-list option is enabled moved from 1.8.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.7.4 - Ensure GDM screen locks when the user is idle moved from 1.8.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.7.5 - Ensure GDM screen locks cannot be overridden moved from 1.8.5 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.7.6 - Ensure GDM automatic mounting of removable media is disabled moved from 1.8.6 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.7.7 - Ensure GDM disabling automatic mounting of removable media is not overridden moved from 1.8.7 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.7.8 - Ensure GDM autorun-never is enabled moved from 1.8.8 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.7.9 - Ensure GDM autorun-never is not overridden moved from 1.8.9 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 1.7.10 - Ensure XDCMP is not enabled moved from 1.8.10 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.1.21 - Ensure mail transfer agent is configured for local-only mode moved from 2.2.15 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.2.1 - Ensure NIS Client is not installed moved from 2.3.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.2.2 - Ensure rsh client is not installed moved from 2.3.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.2.3 - Ensure talk client is not installed moved from 2.3.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.2.4 - Ensure telnet client is not installed moved from 2.3.4 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 2.3 - Configure Time Synchronization moved from 2.1 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 2.3.1 - Ensure time synchronization is in use moved from 2.1.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.3.1.1 - Ensure a single time synchronization daemon is in use moved from 2.1.1.1 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 2.3.2 - Configure systemd-timesyncd moved from 2.1.3 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.3.2.1 - Ensure systemd-timesyncd configured with authorized timeserver moved from 2.1.3.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.3.2.2 - Ensure systemd-timesyncd is enabled and running moved from 2.1.3.2 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 2.3.3 - Configure chrony moved from 2.1.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.3.3.1 - Ensure chrony is configured with authorized timeserver moved from 2.1.2.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.3.3.2 - Ensure chrony is running as user _chrony moved from 2.1.2.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.3.3.3 - Ensure chrony is enabled and running moved from 2.1.2.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.4.1.2 - Ensure permissions on /etc/crontab are configured moved from 5.1.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.4.1.3 - Ensure permissions on /etc/cron.hourly are configured moved from 5.1.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.4.1.4 - Ensure permissions on /etc/cron.daily are configured moved from 5.1.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.4.1.5 - Ensure permissions on /etc/cron.weekly are configured moved from 5.1.5 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.4.1.6 - Ensure permissions on /etc/cron.monthly are configured moved from 5.1.6 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.4.1.7 - Ensure permissions on /etc/cron.d are configured moved from 5.1.7 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 2.4.2.1 - Ensure at is restricted to authorized users moved from 5.1.9 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 3.3.2 - Ensure packet redirect sending is disabled moved from 3.2.1 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED RECOMMENDATION: 3.3.8 - Ensure source routed packets are not accepted moved from 3.3.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 3.3.9 - Ensure suspicious packets are logged moved from 3.3.4 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 4.1 - Configure UncomplicatedFirewall moved from 3.5.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.1.1 - Ensure ufw is installed moved from 3.5.1.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.1.2 - Ensure iptables-persistent is not installed with ufw moved from 3.5.1.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.1.3 - Ensure ufw service is enabled moved from 3.5.1.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.1.4 - Ensure ufw loopback traffic is configured moved from 3.5.1.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.1.5 - Ensure ufw outbound connections are configured moved from 3.5.1.5 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.1.6 - Ensure ufw firewall rules exist for all open ports moved from 3.5.1.6 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.1.7 - Ensure ufw default deny firewall policy moved from 3.5.1.7 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 4.2 - Configure nftables moved from 3.5.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.2.1 - Ensure nftables is installed moved from 3.5.2.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.2.2 - Ensure ufw is uninstalled or disabled with nftables moved from 3.5.2.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.2.3 - Ensure iptables are flushed with nftables moved from 3.5.2.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.2.4 - Ensure a nftables table exists moved from 3.5.2.4 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.2.5 - Ensure nftables base chains exist moved from 3.5.2.5 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.2.6 - Ensure nftables loopback traffic is configured moved from 3.5.2.6 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.2.7 - Ensure nftables outbound and established connections are configured moved from 3.5.2.7 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.2.8 - Ensure nftables default deny firewall policy moved from 3.5.2.8 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.2.9 - Ensure nftables service is enabled moved from 3.5.2.9 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.2.10 - Ensure nftables rules are permanent moved from 3.5.2.10 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 4.3 - Configure iptables moved from 3.5.3 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 4.3.1 - Configure iptables software moved from 3.5.3.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.3.1.1 - Ensure iptables packages are installed moved from 3.5.3.1.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.3.1.2 - Ensure nftables is not installed with iptables moved from 3.5.3.1.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.3.1.3 - Ensure ufw is uninstalled or disabled with iptables moved from 3.5.3.1.3 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 4.3.2 - Configure IPv4 iptables moved from 3.5.3.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.3.2.1 - Ensure iptables default deny firewall policy moved from 3.5.3.2.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.3.2.2 - Ensure iptables loopback traffic is configured moved from 3.5.3.2.2 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.3.2.3 - Ensure iptables outbound and established connections are configured moved from 3.5.3.2.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.3.2.4 - Ensure iptables firewall rules exist for all open ports moved from 3.5.3.2.4 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 4.3.3 - Configure IPv6 ip6tables moved from 3.5.3.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.3.3.1 - Ensure ip6tables default deny firewall policy moved from 3.5.3.3.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.3.3.2 - Ensure ip6tables loopback traffic is configured moved from 3.5.3.3.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.3.3.3 - Ensure ip6tables outbound and established connections are configured moved from 3.5.3.3.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 4.3.3.4 - Ensure ip6tables firewall rules exist for all open ports moved from 3.5.3.3.4 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 5.1 - Configure SSH Server moved from 5.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 5.1.1 - Ensure permissions on /etc/ssh/sshd_config are configured moved from 5.2.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 5.1.2 - Ensure permissions on SSH private host key files are configured moved from 5.2.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 5.1.3 - Ensure permissions on SSH public host key files are configured moved from 5.2.3 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 5.2 - Configure privilege escalation moved from 5.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 5.2.1 - Ensure sudo is installed moved from 5.3.1 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED RECOMMENDATION: 5.2.2 - Ensure sudo commands use pty moved from 5.3.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 5.2.3 - Ensure sudo log file exists moved from 5.3.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 5.2.4 - Ensure users must provide password for privilege escalation moved from 5.3.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 5.2.5 - Ensure re-authentication for privilege escalation is not disabled globally moved from 5.3.5 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 5.2.6 - Ensure sudo authentication timeout is configured correctly moved from 5.3.6 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 5.2.7 - Ensure access to the su command is restricted moved from 5.3.7 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 5.4 - User Accounts and Environment moved from 5.5 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 5.4.1.6 - Ensure all users last password change date is in the past moved from 5.5.1.5 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 5.4.2.1 - Ensure root is the only UID 0 account moved from 6.2.10 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 6 - Logging and Auditing moved from 4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.1.1 - Ensure AIDE is installed moved from 1.3.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.1.2 - Ensure filesystem integrity is regularly checked moved from 1.3.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.1.3 - Ensure cryptographic mechanisms are used to protect the integrity of audit tools moved from 4.1.4.11 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED SECTION: 6.2.1 - Configure journald moved from 4.2.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.2.1.2.1 - Ensure systemd-journal-remote is installed moved from 4.2.1.1.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.1.2 - Ensure auditd service is enabled and active moved from 4.1.1.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.1.3 - Ensure auditing for processes that start prior to auditd is enabled moved from 4.1.1.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.1.4 - Ensure audit_backlog_limit is sufficient moved from 4.1.1.4 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 6.4.2 - Configure Data Retention moved from 4.1.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.2.1 - Ensure audit log storage size is configured moved from 4.1.2.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.2.2 - Ensure audit logs are not automatically deleted moved from 4.1.2.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.2.3 - Ensure system is disabled when audit logs are full moved from 4.1.2.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.1 - Ensure changes to system administration scope (sudoers) is collected moved from 4.1.3.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.2 - Ensure actions as another user are always logged moved from 4.1.3.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.3 - Ensure events that modify the sudo log file are collected moved from 4.1.3.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.4 - Ensure events that modify date and time information are collected moved from 4.1.3.4 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.5 - Ensure events that modify the system's network environment are collected moved from 4.1.3.5 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.6 - Ensure use of privileged commands are collected moved from 4.1.3.6 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.7 - Ensure unsuccessful file access attempts are collected moved from 4.1.3.7 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.8 - Ensure events that modify user/group information are collected moved from 4.1.3.8 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.9 - Ensure discretionary access control permission modification events are collected moved from 4.1.3.9 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.10 - Ensure successful file system mounts are collected moved from 4.1.3.10 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.11 - Ensure session initiation information is collected moved from 4.1.3.11 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.12 - Ensure login and logout events are collected moved from 4.1.3.12 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.13 - Ensure file deletion events by users are collected moved from 4.1.3.13 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.14 - Ensure events that modify the system's Mandatory Access Controls are collected moved from 4.1.3.14 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.15 - Ensure successful and unsuccessful attempts to use the chcon command are recorded moved from 4.1.3.15 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.16 - Ensure successful and unsuccessful attempts to use the setfac command are recorded moved from 4.1.3.16 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.17 - Ensure successful and unsuccessful attempts to use the chacl command are recorded moved from 4.1.3.17 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.18 - Ensure successful and unsuccessful attempts to use the usermod command are recorded moved from 4.1.3.18 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.19 - Ensure kernel module loading unloading and modification is collected moved from 4.1.3.19 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.20 - Ensure the audit configuration is immutable moved from 4.1.3.20 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 6.4.3.21 - Ensure the running and on disk configuration is the same moved from 4.1.3.21 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 7 - System Maintenance moved from 6 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 7.1 - System File Permissions moved from 6.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.1.1 - Ensure permissions on /etc/passwd are configured moved from 6.1.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.1.2 - Ensure permissions on /etc/passwd- are configured moved from 6.1.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.1.3 - Ensure permissions on /etc/group are configured moved from 6.1.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.1.4 - Ensure permissions on /etc/group- are configured moved from 6.1.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.1.5 - Ensure permissions on /etc/shadow are configured moved from 6.1.5 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.1.6 - Ensure permissions on /etc/shadow- are configured moved from 6.1.6 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.1.7 - Ensure permissions on /etc/gshadow are configured moved from 6.1.7 in 1.0.0

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.1.8 - Ensure permissions on /etc/gshadow- are configured moved from 6.1.8 in 1.0.0
3/29/2024	2.0.0	MOVED SECTION: 7.2 - Local User and Group Settings moved from 6.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.2.1 - Ensure accounts in /etc/passwd use shadowed passwords moved from 6.2.1 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.2.2 - Ensure /etc/shadow password fields are not empty moved from 6.2.2 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.2.3 - Ensure all groups in /etc/passwd exist in /etc/group moved from 6.2.3 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.2.4 - Ensure shadow group is empty moved from 6.2.4 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.2.5 - Ensure no duplicate UIDs exist moved from 6.2.5 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.2.6 - Ensure no duplicate GIDs exist moved from 6.2.6 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.2.7 - Ensure no duplicate user names exist moved from 6.2.7 in 1.0.0
3/29/2024	2.0.0	MOVED RECOMMENDATION: 7.2.8 - Ensure no duplicate group names exist moved from 6.2.8 in 1.0.0
<b>UPDATED ITEMS:</b>		
3/29/2024	2.0.0	UPDATED SECTION: 1 - Initial Setup - Sections Modified: Description
3/29/2024	2.0.0	UPDATED SECTION: 1.1.2.1 - Configure /tmp - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.1.1 - Ensure /tmp is a separate partition - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.1.2 - Ensure nodev option set on /tmp partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.1.3 - Ensure nosuid option set on /tmp partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.1.4 - Ensure noexec option set on /tmp partition - Sections Modified: Impact Statement; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED SECTION: 1.1.2.2 - Configure /dev/shm - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.2.2 - Ensure nodev option set on /dev/shm partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.2.3 - Ensure nosuid option set on /dev/shm partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.2.4 - Ensure noexec option set on /dev/shm partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED SECTION: 1.1.2.3 - Configure /home - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.3.1 - Ensure separate partition exists for /home - Sections Modified: Rationale Statement; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.3.2 - Ensure nodev option set on /home partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.3.3 - Ensure nosuid option set on /home partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.4.1 - Ensure separate partition exists for /var - Sections Modified: Rationale Statement; Audit Procedure

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.4.2 - Ensure nodev option set on /var partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.4.3 - Ensure nosuid option set on /var partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.5.1 - Ensure separate partition exists for /var/tmp - Sections Modified: Rationale Statement; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.5.2 - Ensure nodev option set on /var/tmp partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.5.3 - Ensure nosuid option set on /var/tmp partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.5.4 - Ensure noexec option set on /var/tmp partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.6.1 - Ensure separate partition exists for /var/log - Sections Modified: Rationale Statement; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.6.2 - Ensure nodev option set on /var/log partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.6.3 - Ensure nosuid option set on /var/log partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.6.4 - Ensure noexec option set on /var/log partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.7.1 - Ensure separate partition exists for /var/log/audit - Sections Modified: Rationale Statement; Audit Procedure

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.7.2 - Ensure nodev option set on /var/log/audit partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.7.3 - Ensure nosuid option set on /var/log/audit partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.1.2.7.4 - Ensure noexec option set on /var/log/audit partition - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.2.1.1 - Ensure GPG keys are configured - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.2.2.1 - Ensure updates, patches, and additional security software are installed - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED SECTION: 1.3 - Mandatory Access Control - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.3.1.1 - Ensure AppArmor is installed - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.3.1.4 - Ensure all AppArmor Profiles are enforcing - Sections Modified: Remediation Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.4.1 - Ensure bootloader password is set - Sections Modified: Impact Statement; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.5.3 - Ensure core dumps are restricted - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.5.4 - Ensure prelink is not installed - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.5.5 - Ensure Automatic Error Reporting is not enabled - Sections Modified: Remediation Procedure; Audit Procedure

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.6.1 - Ensure message of the day is configured properly - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.6.2 - Ensure local login warning banner is configured properly - Sections Modified: Remediation Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.6.3 - Ensure remote login warning banner is configured properly - Sections Modified: Remediation Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.7.2 - Ensure GDM login banner is configured - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.7.3 - Ensure GDM disable-user-list option is enabled - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.7.4 - Ensure GDM screen locks when the user is idle - Sections Modified: Description; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.7.5 - Ensure GDM screen locks cannot be overridden - Sections Modified: Description; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.7.6 - Ensure GDM automatic mounting of removable media is disabled - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.7.7 - Ensure GDM disabling automatic mounting of removable media is not overridden - Sections Modified: Description; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.7.8 - Ensure GDM autorun-never is enabled - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.7.9 - Ensure GDM autorun-never is not overridden - Sections Modified: Description; Remediation Procedure; Audit Procedure

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 1.7.10 - Ensure XDCMP is not enabled - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED SECTION: 2 - Services - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.1.21 - Ensure mail transfer agent is configured for local-only mode - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.2.1 - Ensure NIS Client is not installed - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.2.2 - Ensure rsh client is not installed - Sections Modified: Rationale Statement; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.2.3 - Ensure talk client is not installed - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.2.4 - Ensure telnet client is not installed - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED SECTION: 2.3 - Configure Time Synchronization - Sections Modified: Description
3/29/2024	2.0.0	UPDATED SECTION: 2.3.1 - Ensure time synchronization is in use - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.3.1.1 - Ensure a single time synchronization daemon is in use - Sections Modified: Description; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED SECTION: 2.3.2 - Configure systemd-timesyncd - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.3.2.1 - Ensure systemd-timesyncd configured with authorized timeserver - Sections Modified: Assessment Status; Remediation Procedure; Audit Procedure

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.3.2.2 - Ensure systemd-timesyncd is enabled and running - Sections Modified: Assessment Status; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED SECTION: 2.3.3 - Configure chrony - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.3.3.1 - Ensure chrony is configured with authorized timeserver - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.3.3.2 - Ensure chrony is running as user _chrony - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.3.3.3 - Ensure chrony is enabled and running - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.4.1.2 - Ensure permissions on /etc/crontab are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.4.1.3 - Ensure permissions on /etc/cron.hourly are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.4.1.4 - Ensure permissions on /etc/cron.daily are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.4.1.5 - Ensure permissions on /etc/cron.weekly are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.4.1.6 - Ensure permissions on /etc/cron.monthly are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.4.1.7 - Ensure permissions on /etc/cron.d are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 2.4.2.1 - Ensure at is restricted to authorized users - Sections Modified: Description; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 3.1.2 - Ensure wireless interfaces are disabled - Sections Modified: Profile; Description; Rationale Statement; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 3.3.2 - Ensure packet redirect sending is disabled - Sections Modified: Impact Statement; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 3.3.8 - Ensure source routed packets are not accepted - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 3.3.9 - Ensure suspicious packets are logged - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED SECTION: 4.1 - Configure UncomplicatedFirewall - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.1.1 - Ensure ufw is installed - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.1.2 - Ensure iptables-persistent is not installed with ufw - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.1.3 - Ensure ufw service is enabled - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.1.5 - Ensure ufw outbound connections are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.1.6 - Ensure ufw firewall rules exist for all open ports - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.1.7 - Ensure ufw default deny firewall policy - Sections Modified: Description; Impact Statement; Remediation Procedure
3/29/2024	2.0.0	UPDATED SECTION: 4.2 - Configure nftables - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.2.1 - Ensure nftables is installed - Sections Modified: Description; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.2.2 - Ensure ufw is uninstalled or disabled with nftables - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.2.6 - Ensure nftables loopback traffic is configured - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED SECTION: 4.3 - Configure iptables - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.3.1.1 - Ensure iptables packages are installed - Sections Modified: Description; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.3.1.2 - Ensure nftables is not installed with iptables - Sections Modified: Description; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.3.1.3 - Ensure ufw is uninstalled or disabled with iptables - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED SECTION: 4.3.2 - Configure IPv4 iptables - Sections Modified: Description
3/29/2024	2.0.0	UPDATED SECTION: 4.3.3 - Configure IPv6 ip6tables - Sections Modified: Description

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.3.3.1 - Ensure ip6tables default deny firewall policy - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.3.3.2 - Ensure ip6tables loopback traffic is configured - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 4.3.3.3 - Ensure ip6tables outbound and established connections are configured - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED SECTION: 5.1 - Configure SSH Server - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 5.1.1 - Ensure permissions on /etc/ssh/sshd_config are configured - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 5.1.2 - Ensure permissions on SSH private host key files are configured - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 5.1.3 - Ensure permissions on SSH public host key files are configured - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED SECTION: 5.2 - Configure privilege escalation - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 5.2.1 - Ensure sudo is installed - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 5.2.2 - Ensure sudo commands use pty - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 5.2.3 - Ensure sudo log file exists - Sections Modified: Remediation Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 5.4.1.6 - Ensure all users last password change date is in the past - Sections Modified: Rationale Statement; Audit Procedure

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 5.4.2.1 - Ensure root is the only UID 0 account - Sections Modified: Remediation Procedure
3/29/2024	2.0.0	UPDATED SECTION: 6 - Logging and Auditing - Sections Modified: Description
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.1.1 - Ensure AIDE is installed - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.1.2 - Ensure filesystem integrity is regularly checked - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.1.3 - Ensure cryptographic mechanisms are used to protect the integrity of audit tools - Sections Modified: Profile; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.2.1.2.1 - Ensure systemd-journal-remote is installed - Sections Modified: Description; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.1.2 - Ensure auditd service is enabled and active - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.2.3 - Ensure system is disabled when audit logs are full - Sections Modified: Description; Impact Statement; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.1 - Ensure changes to system administration scope (sudoers) is collected - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.2 - Ensure actions as another user are always logged - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.3 - Ensure events that modify the sudo log file are collected - Sections Modified: Remediation Procedure; Audit Procedure

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.4 - Ensure events that modify date and time information are collected - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.5 - Ensure events that modify the system's network environment are collected - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.6 - Ensure use of privileged commands are collected - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.7 - Ensure unsuccessful file access attempts are collected - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.8 - Ensure events that modify user/group information are collected - Sections Modified: Description; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.9 - Ensure discretionary access control permission modification events are collected - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.10 - Ensure successful file system mounts are collected - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.11 - Ensure session initiation information is collected - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.12 - Ensure login and logout events are collected - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.13 - Ensure file deletion events by users are collected - Sections Modified: Remediation Procedure; Audit Procedure

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.14 - Ensure events that modify the system's Mandatory Access Controls are collected - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.15 - Ensure successful and unsuccessful attempts to use the chcon command are recorded - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.16 - Ensure successful and unsuccessful attempts to use the setfacl command are recorded - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.17 - Ensure successful and unsuccessful attempts to use the chacl command are recorded - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.18 - Ensure successful and unsuccessful attempts to use the usermod command are recorded - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.19 - Ensure kernel module loading unloading and modification is collected - Sections Modified: Description; Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.20 - Ensure the audit configuration is immutable - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 6.4.3.21 - Ensure the running and on disk configuration is the same - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.1.1 - Ensure permissions on /etc/passwd are configured - Sections Modified: Audit Procedure

<b>Date</b>	<b>Version</b>	<b>Changes for this version</b>
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.1.2 - Ensure permissions on /etc/passwd- are configured - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.1.3 - Ensure permissions on /etc/group are configured - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.1.4 - Ensure permissions on /etc/group- are configured - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.1.5 - Ensure permissions on /etc/shadow are configured - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.1.6 - Ensure permissions on /etc/shadow- are configured - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.1.7 - Ensure permissions on /etc/gshadow are configured - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.1.8 - Ensure permissions on /etc/gshadow- are configured - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.2.1 - Ensure accounts in /etc/passwd use shadowed passwords - Sections Modified: Remediation Procedure; Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.2.3 - Ensure all groups in /etc/passwd exist in /etc/group - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.2.4 - Ensure shadow group is empty - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.2.5 - Ensure no duplicate UIDs exist - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.2.6 - Ensure no duplicate GIDs exist - Sections Modified: Audit Procedure

Date	Version	Changes for this version
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.2.7 - Ensure no duplicate user names exist - Sections Modified: Audit Procedure
3/29/2024	2.0.0	UPDATED RECOMMENDATION: 7.2.8 - Ensure no duplicate group names exist - Sections Modified: Audit Procedure