



# CIS Debian Linux 11 STIG Benchmark

v1.0.0 - 08-31-2023

# Terms of Use

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

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

DRAFT

# Table of Contents

<b>Terms of Use .....</b>	<b>1</b>
<b>Table of Contents .....</b>	<b>2</b>
<b>Overview .....</b>	<b>12</b>
<b>Intended Audience .....</b>	<b>13</b>
<b>Typographical Conventions .....</b>	<b>14</b>
<b>Recommendation Definitions.....</b>	<b>15</b>
<b>Title .....</b>	<b>15</b>
<b>Assessment Status .....</b>	<b>15</b>
<b>Automated .....</b>	<b>15</b>
<b>Manual.....</b>	<b>15</b>
<b>Profile .....</b>	<b>15</b>
<b>Description.....</b>	<b>15</b>
<b>Rationale Statement .....</b>	<b>15</b>
<b>Impact Statement.....</b>	<b>16</b>
<b>Audit Procedure.</b>	<b>16</b>
<b>Remediation Procedure .....</b>	<b>16</b>
<b>Default Value .....</b>	<b>16</b>
<b>References .....</b>	<b>16</b>
<b>CIS Critical Security Controls® (CIS Controls®) .....</b>	<b>16</b>
<b>Additional Information .....</b>	<b>16</b>
<b>Profile Definitions .....</b>	<b>17</b>
<b>Acknowledgements .....</b>	<b>18</b>
<b>1 Initial Setup .....</b>	<b>19</b>
<b>1.1 Filesystem .....</b>	<b>20</b>
<b>1.1.1 Configure Filesystem Kernel Modules.....</b>	<b>21</b>
1.1.1.1 Ensure cramfs kernel module is not available (Automated) .....	22
1.1.1.2 Ensure freevxfs kernel module is not available (Automated) .....	27
1.1.1.3 Ensure hfs kernel module is not available (Automated) .....	32
1.1.1.4 Ensure hfsplus kernel module is not available (Automated).....	37
1.1.1.5 Ensure jffs2 kernel module is not available (Automated) .....	42
1.1.1.6 Ensure overlayfs kernel module is not available (Automated).....	47
1.1.1.7 Ensure squashfs kernel module is not available (Automated).....	52
1.1.1.8 Ensure udf kernel module is not available (Automated) .....	57
1.1.1.9 Ensure usb-storage kernel module is not available (Automated) .....	62
1.1.1.10 Ensure data-at-rest encryption is enabled (Manual) .....	67
1.1.1.11 Ensure data-at-rest employs cryptographic mechanisms to prevent unauthorized modification (Manual).....	69
1.1.1.12 Ensure sticky bit is set on all world-writable directories (Automated).....	71

<b>1.1.2 Configure Filesystem Partitions .....</b>	<b>73</b>
1.1.2.1 Ensure /tmp is a separate partition (Automated) .....	75
1.1.2.1.2 Ensure nodev option set on /tmp partition (Automated) .....	79
1.1.2.1.3 Ensure nosuid option set on /tmp partition (Automated) .....	81
1.1.2.1.4 Ensure noexec option set on /tmp partition (Automated) .....	83
1.1.2.2.1 Ensure /dev/shm is a separate partition (Automated) .....	86
1.1.2.2.2 Ensure nodev option set on /dev/shm partition (Automated).....	88
1.1.2.2.3 Ensure nosuid option set on /dev/shm partition (Automated).....	90
1.1.2.2.4 Ensure noexec option set on /dev/shm partition (Automated).....	92
1.1.2.3.1 Ensure separate partition exists for /home (Automated) .....	95
1.1.2.3.2 Ensure nodev option set on /home partition (Automated) .....	97
1.1.2.3.3 Ensure nosuid option set on /home partition (Automated) .....	99
1.1.2.4.1 Ensure separate partition exists for /var (Automated) .....	102
1.1.2.4.2 Ensure nodev option set on /var partition (Automated) .....	105
1.1.2.4.3 Ensure nosuid option set on /var partition (Automated) .....	107
1.1.2.5.1 Ensure separate partition exists for /var/tmp (Automated) .....	110
1.1.2.5.2 Ensure nodev option set on /var/tmp partition (Automated) .....	113
1.1.2.5.3 Ensure nosuid option set on /var/tmp partition (Automated) .....	115
1.1.2.5.4 Ensure noexec option set on /var/tmp partition (Automated) .....	117
1.1.2.6.1 Ensure separate partition exists for /var/log (Automated) .....	120
1.1.2.6.2 Ensure nodev option set on /var/log partition (Automated) .....	122
1.1.2.6.3 Ensure nosuid option set on /var/log partition (Automated).....	124
1.1.2.6.4 Ensure noexec option set on /var/log partition (Automated).....	126
1.1.2.7.1 Ensure separate partition exists for /var/log/audit (Automated).....	129
1.1.2.7.2 Ensure nodev option set on /var/log/audit partition (Automated).....	131
1.1.2.7.3 Ensure nosuid option set on /var/log/audit partition (Automated) .....	133
1.1.2.7.4 Ensure noexec option set on /var/log/audit partition (Automated) .....	135
<b>1.2 Configure Software and Patch Management .....</b>	<b>137</b>
1.2.1 Ensure updates, patches, and additional security software are installed (Manual) .....	138
1.2.2 Ensure package manager repositories are configured (Manual).....	141
1.2.3 Ensure GPG keys are configured (Manual) .....	143
1.2.4 Ensure apt is configured to prevent installation without verification of a recognized and approved digital signature (Automated) .....	145
1.2.5 Ensure the Advance Package Tool removes all software components after updated versions have been installed (Automated) .....	147
<b>1.3 Secure Boot Settings.....</b>	<b>149</b>
1.3.1 Ensure bootloader password is set (Automated) .....	150
1.3.2 Ensure permissions on bootloader config are configured (Automated).....	153
1.3.3 Ensure authentication required for single user mode (Automated) .....	155
<b>1.4 Additional Process Hardening .....</b>	<b>157</b>
1.4.1 Ensure XD/NX support is enabled (Manual) .....	158
1.4.2 Ensure address space layout randomization (ASLR) is enabled (Automated).....	160
1.4.3 Ensure ptrace_scope is restricted (Automated) .....	164
1.4.4 Ensure prelink is not installed (Automated).....	168
1.4.5 Ensure maxlogins is 10 or less (Automated).....	170
1.4.6 Ensure Automatic Error Reporting is not enabled (Automated) .....	172
1.4.7 Ensure kdump service is not enabled (Automated).....	174
1.4.8 Ensure core dumps are restricted (Automated) .....	176
1.4.9 Ensure the Ctrl-Alt-Delete key sequence is disabled (Automated).....	179
1.4.10 Ensure dmesg_restrict is enabled (Automated) .....	181
<b>1.5 Mandatory Access Control .....</b>	<b>185</b>
<b>1.5.1 Configure AppArmor .....</b>	<b>186</b>

1.5.1.1 Ensure AppArmor is installed (Automated) .....	187
1.5.1.2 Ensure AppArmor is enabled in the bootloader configuration (Automated).....	189
1.5.1.3 Ensure AppArmor is installed, enabled, and active (Automated) .....	191
1.5.1.4 Ensure all AppArmor Profiles are in enforce or complain mode (Automated) .....	193
1.5.1.5 Ensure all AppArmor Profiles are enforcing (Automated).....	195
<b>1.6 Command Line Warning Banners .....</b>	<b>197</b>
1.6.1 Ensure message of the day is configured properly (Automated).....	198
1.6.2 Ensure local login warning banner is configured properly (Automated) .....	200
1.6.3 Ensure remote login warning banner is configured properly (Automated).....	202
1.6.4 Ensure permissions on /etc/motd are configured (Automated) .....	204
1.6.5 Ensure permissions on /etc/issue are configured (Automated).....	206
1.6.6 Ensure permissions on /etc/issue.net are configured (Automated) .....	208
<b>1.7 GNOME Display Manager.....</b>	<b>210</b>
1.7.1 Ensure GNOME Display Manager is removed (Automated) .....	211
1.7.2 Ensure GDM login banner is configured (Automated).....	213
1.7.3 Ensure GDM disable-user-list option is enabled (Automated).....	217
1.7.4 Ensure GDM screen locks when the user is idle (Automated) .....	221
1.7.5 Ensure GDM screen locks cannot be overridden (Automated) .....	226
1.7.6 Ensure GDM automatic mounting of removable media is disabled (Automated) .....	231
1.7.7 Ensure user's session lock is enabled (Automated).....	238
1.7.8 Ensure GDM disabling automatic mounting of removable media is not overridden (Automated)....	240
1.7.9 Ensure GDM autorun-never is enabled (Automated) .....	245
1.7.10 Ensure GDM autorun-never is not overridden (Automated).....	251
1.7.11 Ensure XDCMP is not enabled (Automated).....	255
1.7.12 Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon (Manual).....	257
1.7.13 Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled (Automated) .....	262
<b>1.8 Additional Software .....</b>	<b>264</b>
1.8.1 Ensure vlock is installed (Automated) .....	265
1.8.2 Ensure Endpoint Security for Linux Threat Prevention is installed (Automated) .....	267
<b>1.9 Federal Information Processing Standards (FIPS) Cryptographic Modules .....</b>	<b>269</b>
<b>2 Services .....</b>	<b>270</b>
<b>2.1 Configure Time Synchronization .....</b>	<b>270</b>
<b>2.1.1 Ensure time synchronization is in use.....</b>	<b>271</b>
2.1.1.1 Ensure a single time synchronization daemon is in use (Automated) .....	272
<b>2.1.2 Configure chrony .....</b>	<b>276</b>
2.1.2.1 Ensure chrony is configured with authorized timeserver (Manual).....	277
2.1.2.2 Ensure chrony is running as user _chrony (Automated) .....	280
2.1.2.3 Ensure chrony is enabled and running (Automated) .....	282
<b>2.1.3 Configure systemd-timesyncd.....</b>	<b>284</b>
2.1.3.1 Ensure systemd-timesyncd configured with authorized timeserver (Automated) .....	286
2.1.3.2 Ensure systemd-timesyncd is enabled and running (Manual).....	290
<b>2.1.4 Configure ntp.....</b>	<b>292</b>
2.1.4.1 Ensure ntp access control is configured (Automated) .....	293
2.1.4.2 Ensure ntp is configured with authorized timeserver (Manual).....	297
2.1.4.3 Ensure ntp is running as user ntp (Automated).....	300
2.1.4.4 Ensure ntp is enabled and running (Automated) .....	302
2.1.5 Ensure system clocks are synchronize to the authoritative time source when the time difference is greater than one second (Automated) .....	304
2.1.6 Ensure system clocks are synchronized with a time server designated for the appropriate DoD network (Automated).....	306
2.1.7 Ensure system timezone is set to UTC or GMT (Automated) .....	309

<b>2.2 Special Purpose Services .....</b>	<b>311</b>
2.2.1 Ensure X Window System is not installed (Automated) .....	312
2.2.2 Ensure Avahi Server is not installed (Automated) .....	314
2.2.3 Ensure CUPS is not installed (Automated) .....	316
2.2.4 Ensure DHCP Server is not installed (Automated) .....	318
2.2.5 Ensure LDAP server is not installed (Automated) .....	320
2.2.6 Ensure NFS is not installed (Automated) .....	322
2.2.7 Ensure DNS Server is not installed (Automated) .....	324
2.2.8 Ensure FTP Server is not installed (Automated) .....	326
2.2.9 Ensure HTTP server is not installed (Automated) .....	328
2.2.10 Ensure IMAP and POP3 server are not installed (Automated) .....	330
2.2.11 Ensure Samba is not installed (Automated) .....	332
2.2.12 Ensure HTTP Proxy Server is not installed (Automated) .....	334
2.2.13 Ensure SNMP Server is not installed (Automated) .....	336
2.2.14 Ensure NIS Server is not installed (Automated) .....	338
2.2.15 Ensure dnsmasq is not installed (Automated) .....	340
2.2.16 Ensure mail transfer agent is configured for local-only mode (Automated) .....	342
2.2.17 Ensure telnetd is not installed (Automated) .....	344
2.2.18 Ensure rsync service is either not installed or is masked (Automated) .....	346
2.2.19 Ensure rsh-server is not installed (Automated) .....	348
<b>2.3 Service Clients .....</b>	<b>350</b>
2.3.1 Ensure NIS Client is not installed (Automated) .....	351
2.3.2 Ensure rsh client is not installed (Automated) .....	353
2.3.3 Ensure talk client is not installed (Automated) .....	355
2.3.4 Ensure telnet client is not installed (Automated) .....	357
2.3.5 Ensure LDAP client is not installed (Automated) .....	359
2.3.6 Ensure RPC is not installed (Automated) .....	361
2.4 Ensure nonessential services are removed or masked (Manual) .....	363
<b>3 Network .....</b>	<b>366</b>
<b>3.1 Configure Network Devices .....</b>	<b>367</b>
3.1.1 Ensure IPv6 status is identified (Manual) .....	368
3.1.2 Ensure wireless interfaces are disabled (Automated) .....	371
3.1.3 Ensure bluetooth services are not in use (Automated) .....	375
<b>3.2 Configure Network Kernel Modules .....</b>	<b>378</b>
3.2.1 Ensure dccp kernel module is not available (Automated) .....	379
3.2.2 Ensure sctp kernel module is not available (Automated) .....	384
3.2.3 Ensure rds kernel module is not available (Automated) .....	389
3.2.4 Ensure tipc kernel module is not available (Automated) .....	394
<b>3.3 Configure Network Kernel Parameters .....</b>	<b>399</b>
3.3.1 Ensure ip forwarding is disabled (Automated) .....	400
3.3.2 Ensure packet redirect sending is disabled (Automated) .....	404
3.3.3 Ensure bogus icmp responses are ignored (Automated) .....	408
3.3.4 Ensure broadcast icmp requests are ignored (Automated) .....	412
3.3.5 Ensure icmp redirects are not accepted (Automated) .....	416
3.3.6 Ensure secure icmp redirects are not accepted (Automated) .....	420
3.3.7 Ensure reverse path filtering is enabled (Automated) .....	424
3.3.8 Ensure tcp syn Cookies is enabled (Automated) .....	428
3.3.9 Ensure source routed packets are not accepted (Automated) .....	433
3.3.10 Ensure suspicious packets are logged (Automated) .....	438
3.3.11 Ensure ipv6 router advertisements are not accepted (Automated) .....	442
<b>3.4 Configure Host Based Firewall.....</b>	<b>446</b>

<b>3.4.1 Configure UncomplicatedFirewall .....</b>	<b>447</b>
3.4.1.1 Ensure ufw is installed (Automated).....	448
3.4.1.2 Ensure iptables-persistent is not installed with ufw (Automated) .....	450
3.4.1.3 Ensure ufw service is enabled (Automated).....	452
3.4.1.4 Ensure ufw loopback traffic is configured (Automated) .....	455
3.4.1.5 Ensure ufw outbound connections are configured (Manual) .....	457
3.4.1.6 Ensure ufw firewall rules exist for all open ports (Automated).....	459
3.4.1.7 Ensure ufw default deny firewall policy (Automated).....	462
3.4.1.8 Ensure UFW rate-limits impacted network interfaces (Manual) .....	464
<b>3.4.2 Configure nftables.....</b>	<b>467</b>
3.4.2.1 Ensure nftables is installed (Automated).....	470
3.4.2.2 Ensure ufw is uninstalled or disabled with nftables (Automated) .....	472
3.4.2.3 Ensure iptables are flushed with nftables (Manual).....	474
3.4.2.4 Ensure a nftables table exists (Automated).....	476
3.4.2.5 Ensure nftables base chains exist (Automated) .....	478
3.4.2.6 Ensure nftables loopback traffic is configured (Automated) .....	480
3.4.2.7 Ensure nftables outbound and established connections are configured (Manual) .....	482
3.4.2.8 Ensure nftables default deny firewall policy (Automated).....	485
3.4.2.9 Ensure nftables service is enabled (Automated).....	488
3.4.2.10 Ensure nftables rules are permanent (Automated) .....	490
<b>3.4.3 Configure iptables.....</b>	<b>494</b>
3.4.3.1.1 Ensure iptables packages are installed (Automated) .....	496
3.4.3.1.2 Ensure nftables is not installed with iptables (Automated) .....	498
3.4.3.1.3 Ensure ufw is uninstalled or disabled with iptables (Automated).....	500
3.4.3.2.1 Ensure iptables default deny firewall policy (Automated) .....	503
3.4.3.2.2 Ensure iptables loopback traffic is configured (Automated) .....	505
3.4.3.2.3 Ensure iptables outbound and established connections are configured (Manual) .....	507
3.4.3.2.4 Ensure iptables firewall rules exist for all open ports (Automated) .....	509
3.4.3.3.1 Ensure ip6tables default deny firewall policy (Automated) .....	513
3.4.3.3.2 Ensure ip6tables loopback traffic is configured (Automated) .....	515
3.4.3.3.3 Ensure ip6tables outbound and established connections are configured (Manual) .....	518
3.4.3.3.4 Ensure ip6tables firewall rules exist for all open ports (Automated) .....	520
<b>4 Access, Authentication and Authorization .....</b>	<b>523</b>
<b>4.1 Configure job schedulers .....</b>	<b>524</b>
<b>4.1.1 Configure cron.....</b>	<b>525</b>
4.1.1.1 Ensure cron daemon is enabled and active (Automated).....	526
4.1.1.2 Ensure permissions on /etc/crontab are configured (Automated) .....	527
4.1.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated).....	529
4.1.1.4 Ensure permissions on /etc/cron.daily are configured (Automated) .....	531
4.1.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated) .....	533
4.1.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated) .....	535
4.1.1.7 Ensure permissions on /etc/cron.d are configured (Automated) .....	537
4.1.1.8 Ensure crontab is restricted to authorized users (Automated) .....	539
<b>4.1.2 Configure at .....</b>	<b>543</b>
4.1.2.1 Ensure at is restricted to authorized users (Automated) .....	544
<b>4.2 Configure SSH Server .....</b>	<b>548</b>
4.2.1 Ensure SSH is installed and active (Automated).....	550
4.2.2 Ensure permissions on /etc/ssh/sshd_config are configured (Automated) .....	553
4.2.3 Ensure permissions on SSH private host key files are configured (Automated) .....	556
4.2.4 Ensure permissions on SSH public host key files are configured (Automated).....	560
4.2.5 Ensure SSH access is limited (Automated).....	564

4.2.6 Ensure SSH LogLevel is appropriate (Automated) .....	567
4.2.7 Ensure SSH PAM is enabled (Automated).....	569
4.2.8 Ensure SSH root login is disabled (Automated) .....	571
4.2.9 Ensure SSH HostbasedAuthentication is disabled (Automated) .....	573
4.2.10 Ensure SSH PermitEmptyPasswords is disabled (Automated).....	575
4.2.11 Ensure SSH PermitUserEnvironment is disabled (Automated).....	577
4.2.12 Ensure SSH IgnoreRhosts is enabled (Automated) .....	579
4.2.13 Ensure SSH X11 forwarding is disabled (Automated).....	581
4.2.14 Ensure only strong Ciphers are used (Automated) .....	583
4.2.15 Ensure only strong MAC algorithms are used (Automated) .....	585
4.2.16 Ensure only strong Key Exchange algorithms are used (Automated) .....	588
4.2.17 Ensure SSH AllowTcpForwarding is disabled (Automated) .....	591
4.2.18 Ensure SSH warning banner is configured (Automated).....	593
4.2.19 Ensure SSH MaxAuthTries is set to 4 or less (Automated).....	594
4.2.20 Ensure SSH MaxStartups is configured (Automated) .....	596
4.2.21 Ensure SSH LoginGraceTime is set to one minute or less (Automated).....	598
4.2.22 Ensure SSH MaxSessions is set to 10 or less (Automated).....	600
4.2.23 Ensure SSH Idle Timeout Interval is configured (Automated) .....	602
4.2.24 Ensure network connections associated with SSH traffic are terminated after a period of inactivity (Automated) .....	605
4.2.25 Ensure network connections associated with SSH traffic are terminated at the end of the session or 10 minutes of inactivity (Automated).....	607
4.2.26 Ensure Standard Mandatory DoD Notice and Consent Banner displayed before granting any local or remote connection to the system (Manual).....	609
4.2.27 Ensure only FIPS validated MAC algorithms are used (Automated).....	613
4.2.28 Ensure only FIPS validated Ciphers are used (Automated).....	616
4.2.29 Ensure only FIPS validated Key Exchange algorithms are used (Automated).....	619
4.2.30 Ensure X11UseLocalhost is enabled (Automated).....	621
<b>4.3 Configure privilege escalation .....</b>	<b>623</b>
4.3.1 Ensure sudo is installed (Automated).....	624
4.3.2 Ensure sudo commands use pty (Automated) .....	626
4.3.3 Ensure sudo log file exists (Automated) .....	628
4.3.4 Ensure only users who need access to security functions are part of sudo group (Manual) .....	630
4.3.5 Ensure users must provide password for privilege escalation (Automated).....	632
4.3.6 Ensure re-authentication for privilege escalation is not disabled globally (Automated) .....	634
4.3.7 Ensure sudo authentication timeout is configured correctly (Automated).....	636
4.3.8 Ensure access to the su command is restricted (Automated) .....	638
<b>4.4 Configure Pluggable Authentication Modules.....</b>	<b>640</b>
<b>    4.4.1 Configure pam_pwquality module .....</b>	<b>641</b>
4.4.1.1 Ensure new and changed passwords use pwquality (Automated) .....	642
4.4.1.2 Ensure password creation requirements are configured (Automated) .....	644
4.4.1.3 Ensure maximum number of same consecutive characters in a password is configured (Automated) .....	648
4.4.1.4 Ensure the number of changed characters in a new password is configured (Automated).....	650
4.4.1.5 Ensure preventing the use of dictionary words for passwords is configured (Automated) .....	652
4.4.1.6 Ensure password includes at least one upper-case character (Automated) .....	654
4.4.1.7 Ensure password includes at least one lower-case character (Automated).....	656
4.4.1.8 Ensure password includes at least one numeric character (Automated).....	658
4.4.1.9 Ensure password includes at least one special character (Automated) .....	660
4.4.1.10 Ensure change of at least 8 characters when passwords are changed (Automated).....	662
4.4.1.11 Ensure password is at least 15 characters (Automated) .....	664
<b>    4.4.2 Configure pam_pwhistory module .....</b>	<b>666</b>
4.4.2.1 Ensure password reuse is limited (Automated) .....	668

<b>4.4.3 Configure pam_faillock module.....</b>	<b>671</b>
4.4.3.1 Ensure lockout for failed password attempts is configured (Automated).....	673
4.4.3.2 Ensure lockout for three or more failed password attempts is configured (Automated) .....	677
<b>4.4.4 Configure pam_unix module.....</b>	<b>681</b>
4.4.4.1 Ensure strong password hashing algorithm is configured (Automated).....	682
4.4.4.2 Ensure pam modules do not include nullok (Automated).....	685
<b>4.4.5 Configure System Security Services .....</b>	<b>687</b>
4.4.5.1 Ensure PAM prohibits the use of cached authentications after one day (Automated).....	688
<b>4.4.6 Configure pam_pkcs11 module.....</b>	<b>690</b>
4.4.6.1 Ensure the libpam-pkcs11 package is installed (Automated).....	691
4.4.6.2 Ensure the opensc-pkcs11 is installed (Automated) .....	693
4.4.6.3 Ensure authenticated identity is mapped to the user or group account for PKI-based authentication (Automated) .....	695
4.4.6.4 Ensure smart card logins for multifactor authentication for local and network access (Automated) .....	697
4.4.6.5 Ensure certificates are validated by constructing a certification path to an accepted trust anchor (Automated) .....	700
4.4.6.6 Ensure Personal Identity Verification credentials are electronically verified (Automated) .....	702
4.4.6.7 Ensure PKI local cache of revocation data (Automated).....	704
<b>4.4.7 Configure pam_lastlog module .....</b>	<b>706</b>
4.4.7.1 Ensure last successful account logon is displayed upon logon (Automated) .....	707
<b>4.4.8 Configure pam_faildelay .....</b>	<b>709</b>
4.4.8.1 Ensure login delay after failed logon attempt (Automated).....	710
4.4.9 Ensure all current passwords uses the configured hashing algorithm (Manual) .....	712
<b>4.5 User Accounts and Environment.....</b>	<b>714</b>
<b>4.5.1 Set Shadow Password Suite Parameters .....</b>	<b>715</b>
4.5.1.1 Ensure minimum days between password changes is configured (Automated) .....	716
4.5.1.2 Ensure password expiration is 365 days or less (Automated).....	718
4.5.1.3 Ensure password expiration warning days is 7 or more (Automated) .....	720
4.5.1.4 Ensure inactive password lock is 30 days or less (Automated).....	722
4.5.1.5 Ensure all users last password change date is in the past (Automated) .....	724
4.5.1.6 Ensure ENCRYPT_METHOD is SHA512 (Automated).....	726
4.5.1.7 Ensure temporary accounts expiration time of 72 hours or less (Manual).....	728
4.5.1.8 Ensure root account is locked (Automated) .....	730
4.5.1.9 Ensure password expiration is 60 days or less (Automated).....	732
4.5.1.10 Ensure emergency accounts are removed or disabled after 72 hours (Manual) .....	734
4.5.1.11 Ensure immediate change to a permanent password (Manual) .....	736
4.5.2 Ensure system accounts are secured (Automated) .....	738
4.5.3 Ensure default group for the root account is GID 0 (Automated) .....	742
4.5.4 Ensure default user umask is 027 or more restrictive (Automated).....	744
4.5.5 Ensure default user shell timeout is configured (Automated) .....	749
4.5.6 Ensure default user umask is 077 or more restrictive (Automated).....	754
4.5.7 Ensure nologin is not listed in /etc/shells (Automated).....	756
4.5.8 Ensure default user shell timeout is 600 seconds or less (Automated) .....	757
4.6 Ensure /etc/ssl/certs only contains certificate files whose sha256 fingerprint match the fingerprint of Dod PKI-established certificate authorities (Automated) .....	760
<b>5 Logging and Auditing .....</b>	<b>762</b>
<b>5.1 Configure Logging.....</b>	<b>763</b>
<b>5.1.1 Configure journald .....</b>	<b>764</b>
5.1.1.1 Ensure systemd-journal-remote is installed (Automated).....	766
5.1.1.2 Ensure systemd-journal-remote is configured (Manual).....	768
5.1.1.3 Ensure systemd-journal-remote is enabled (Manual).....	770

5.1.1.1.4 Ensure journald is not configured to receive logs from a remote client (Automated).....	772
5.1.1.2 Ensure journald service is enabled (Automated).....	774
5.1.1.3 Ensure journald is configured to compress large log files (Automated).....	776
5.1.1.4 Ensure journald is configured to write logfiles to persistent disk (Automated).....	778
5.1.1.5 Ensure journald is not configured to send logs to rsyslog (Manual) .....	780
5.1.1.6 Ensure journald log rotation is configured per site policy (Manual) .....	782
5.1.1.7 Ensure journald default file permissions configured (Manual).....	784
<b>5.1.2 Configure rsyslog.....</b>	<b>786</b>
5.1.2.1 Ensure rsyslog is installed (Automated).....	787
5.1.2.2 Ensure rsyslog service is enabled (Automated).....	789
5.1.2.3 Ensure journald is configured to send logs to rsyslog (Manual) .....	791
5.1.2.4 Ensure rsyslog default file permissions are configured (Automated) .....	794
5.1.2.5 Ensure logging is configured (Manual).....	797
5.1.2.6 Ensure rsyslog is configured to send logs to a remote log host (Manual) .....	799
5.1.2.7 Ensure remote access methods are monitored (Automated) .....	801
5.1.2.8 Ensure rsyslog is not configured to receive logs from a remote client (Automated) .....	803
<b>5.1.3 Configure logfile access.....</b>	<b>806</b>
5.1.3.1 Ensure /var/log is owned by root (Automated) .....	807
5.1.3.2 Ensure /var/log is group-owned by syslog (Automated) .....	809
5.1.3.3 Ensure /var/log is mode 0755 or more restrictive (Automated) .....	811
5.1.3.4 Ensure all logfiles have appropriate access configured (Automated).....	813
5.1.3.5 Ensure /var/log/syslog is owned by syslog (Automated) .....	820
5.1.3.6 Ensure /var/log/syslog is group-owned by adm (Automated) .....	822
5.1.3.7 Ensure /var/log/syslog is 0640 or more restrictive (Automated) .....	824
<b>5.2 Configure System Accounting (auditd).....</b>	<b>826</b>
<b>5.2.1 Ensure auditing is enabled .....</b>	<b>828</b>
5.2.1.1 Ensure auditd is installed (Automated).....	829
5.2.1.2 Ensure auditd service is enabled and active (Automated) .....	831
5.2.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated) .....	833
5.2.1.4 Ensure audit_backlog_limit is sufficient (Automated) .....	835
<b>5.2.2 Configure Data Retention .....</b>	<b>837</b>
5.2.2.1 Ensure audit log storage size is configured (Automated) .....	838
5.2.2.2 Ensure audit logs are not automatically deleted (Automated) .....	840
5.2.2.3 Ensure system is disabled when audit logs are full (Automated) .....	842
5.2.2.4 Ensure crontab scrip running to offload audit events of standalone systems (Manual).....	844
5.2.2.5 Ensure shut down by default upon audit failure (Automated) .....	846
5.2.2.6 Ensure security personnel are notified when storage volume reaches 75 percent utilization (Manual).....	848
5.2.2.7 Ensure sufficient storage capacity to store at least one week worth of audit records (Manual) .....	850
5.2.2.8 Ensure audit event multiplexor is configured to off-load audit logs onto a different system or storage media from the system being audited).....	852
<b>5.2.3 Configure auditd rules .....</b>	<b>854</b>
5.2.3.1 Ensure changes to system administration scope (sudoers) is collected (Automated).....	855
5.2.3.2 Ensure actions as another user are always logged (Automated) .....	858
5.2.3.3 Ensure events that modify the sudo log file are collected (Automated) .....	862
5.2.3.4 Ensure events that modify date and time information are collected (Automated) .....	866
5.2.3.5 Ensure events that modify the system's network environment are collected (Automated).....	870
5.2.3.6 Ensure use of privileged commands are collected (Automated) .....	874
5.2.3.7 Ensure unsuccessful file access attempts are collected (Automated) .....	878
5.2.3.8 Ensure events that modify user/group information are collected (Automated) .....	882
5.2.3.9 Ensure discretionary access control permission modification events are collected (Automated) .....	886
5.2.3.10 Ensure successful file system mounts are collected (Automated) .....	890

5.2.3.11 Ensure session initiation information is collected (Automated) .....	894
5.2.3.12 Ensure login and logout events are collected (Automated) .....	898
5.2.3.13 Ensure file deletion events by users are collected (Automated).....	901
5.2.3.14 Ensure events that modify the system's Mandatory Access Controls are collected (Automated).....	905
5.2.3.15 Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated) .....	908
5.2.3.16 Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated) .....	912
5.2.3.17 Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated) .....	916
5.2.3.18 Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated) .....	920
5.2.3.19 Ensure kernel module loading unloading and modification is collected (Automated).....	924
5.2.3.20 Ensure successful and unsuccessful uses of the su command are collected (Automated).....	929
5.2.3.21 Ensure successful and unsuccessful uses of the chfn command are collected (Automated).....	931
5.2.3.22 Ensure successful and unsuccessful uses of the ssh-agent command are collected (Automated) .....	933
5.2.3.23 Ensure successful and unsuccessful uses of the ssh-keysign command are collected (Automated) .....	935
5.2.3.24 Ensure successful and unsuccessful attempts to use the fdisk command are recorded (Automated) .....	937
5.2.3.25 Ensure successful and unsuccessful uses of the sudo command are recorded (Automated)....	939
5.2.3.26 Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are recorded (Automated) .....	941
5.2.3.27 Ensure successful and unsuccessful attempts to use the sudoedit command are recorded (Automated) .....	943
5.2.3.28 Ensure successful and unsuccessful attempts to use the crontab command are recorded (Automated) .....	945
5.2.3.29 Ensure successful and unsuccessful attempts to use the chsh command are recorded (Automated) .....	947
5.2.3.30 Ensure successful and unsuccessful attempts to use the chage command are recorded (Automated) .....	949
5.2.3.31 Ensure successful and unsuccessful attempts to use the newgrp command are recorded (Automated) .....	951
5.2.3.32 Ensure successful and unsuccessful attempts to use the gpasswd command are recorded (Automated) .....	953
5.2.3.33 Ensure successful and unsuccessful attempts to use the unix_update command are recorded (Automated) .....	955
5.2.3.34 Ensure successful and unsuccessful attempts to use the apparmor_parser command are recorded (Automated) .....	957
5.2.3.35 Ensure successful and unsuccessful attempts to use the passwd command are recorded (Automated) .....	959
5.2.3.36 Ensure the running and on disk configuration is the same (Manual).....	961
5.2.3.37 Ensure the audit configuration is immutable (Automated).....	963
<b>5.2.4 Configure auditd file access .....</b>	<b>965</b>
5.2.4.1 Ensure the audit log directory is 0750 or more restrictive (Automated).....	966
5.2.4.2 Ensure audit log files are mode 0640 or more restrictive (Automated).....	968
5.2.4.3 Ensure audit log files are mode 0600 or more restrictive (Automated).....	970
5.2.4.4 Ensure only authorized users own audit log files (Automated).....	972
5.2.4.5 Ensure only authorized groups own audit log files (Automated) .....	974
5.2.4.6 Ensure audit configuration files are 640 or more restrictive (Automated).....	977
5.2.4.7 Ensure only authorized users own audit configuration files (Automated).....	979
5.2.4.8 Ensure only authorized groups own audit configuration files (Automated) .....	981
5.2.4.9 Ensure audit tools are 755 or more restrictive (Automated) .....	983
5.2.4.10 Ensure only authorized users own audit tools (Automated) .....	985

5.2.4.11 Ensure only authorized groups own audit tools (Automated) .....	988
<b>5.3 Filesystem Integrity Checking .....</b>	<b>991</b>
5.3.1 Ensure AIDE is installed (Automated) .....	992
5.3.2 Ensure aide script to check file integrity is the default (Manual).....	994
5.3.3 Ensure filesystem integrity is regularly checked (Automated) .....	996
5.3.4 Ensure System Administrator are notified of changes to the baseline configuration or anomalies (Automated) .....	999
5.3.5 Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)....	1001
<b>6 System Maintenance .....</b>	<b>1003</b>
<b>6.1 System File Permissions .....</b>	<b>1004</b>
6.1.1 Ensure permissions on /etc/passwd are configured (Automated) .....	1005
6.1.2 Ensure permissions on /etc/passwd- are configured (Automated) .....	1007
6.1.3 Ensure permissions on /etc/group are configured (Automated) .....	1009
6.1.4 Ensure permissions on /etc/group- are configured (Automated).....	1011
6.1.5 Ensure permissions on /etc/shadow are configured (Automated) .....	1013
6.1.6 Ensure permissions on /etc/shadow- are configured (Automated).....	1015
6.1.7 Ensure permissions on /etc/gshadow are configured (Automated).....	1017
6.1.8 Ensure permissions on /etc/gshadow- are configured (Automated).....	1019
6.1.9 Ensure permissions on /etc/shells are configured (Automated) .....	1021
6.1.10 Ensure permissions on /etc/opasswd are configured (Automated) .....	1023
6.1.11 Ensure world writable files and directories are secured (Automated) .....	1025
6.1.12 Ensure no unowned or ungrouped files or directories exist (Automated) .....	1029
6.1.13 Ensure SUID and SGID files are reviewed (Manual) .....	1032
6.1.14 Ensure system command files are group-owned by root (Automated).....	1035
6.1.15 Ensure system command files are owned by root (Automated) .....	1037
6.1.16 Ensure directories that contain system commands set to 0755 or more restrictive (Automated) .....	1039
6.1.17 Ensure system library directories are group-owned by root (Automated).....	1041
6.1.18 Ensure system library files are group-owned by root (Automated).....	1043
6.1.19 Ensure system library directories are owned by root (Automated) .....	1045
6.1.20 Ensure directories that contain system commands are owned by root (Automated).....	1047
6.1.21 Ensure system library files are owned by root (Automated) .....	1049
6.1.22 Ensure directories that contain system commands are group-owned by root (Automated) .....	1051
6.1.23 Ensure system library directories are 0755 or more restrictive (Automated).....	1053
6.1.24 Ensure system library files are 0755 or more restrictive (Automated).....	1055
<b>6.2 Local User and Group Settings .....</b>	<b>1057</b>
6.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated) .....	1058
6.2.2 Ensure /etc/shadow password fields are not empty (Automated) .....	1060
6.2.3 Ensure all groups in /etc/passwd exist in /etc/group (Automated) .....	1062
6.2.4 Ensure shadow group is empty (Automated) .....	1063
6.2.5 Ensure no duplicate UIDs exist (Automated) .....	1065
6.2.6 Ensure no duplicate GIDs exist (Automated) .....	1067
6.2.7 Ensure no duplicate user names exist (Automated).....	1068
6.2.8 Ensure no duplicate group names exist (Automated) .....	1069
6.2.9 Ensure root PATH Integrity (Automated).....	1070
6.2.10 Ensure root is the only UID 0 account (Automated) .....	1072
6.2.11 Ensure local interactive user home directories are configured (Automated) .....	1073
6.2.12 Ensure local interactive user dot files access is configured (Automated).....	1077
<b>Appendix: Summary Table .....</b>	<b>1083</b>
<b>Appendix: Change History .....</b>	<b>1191</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 x64 platforms.

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

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

The STIG profile includes guidance from the publicly available Ubuntu Linux 20.04 LTS STIG. This has been tested against Debian 11 Linux. **"Ensure FIPS mode is enabled" is not able to be applied in this environment due to the required FIPS validated libraries not being available.** Other recommendations may require adding users and/or groups to apply the recommendations.

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 a Debian Linux 11 system on the x64 platform.

### 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.

- **STIG**

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

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

## Acknowledgements

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

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

### **Contributor**

Dave Billing  
Dominic Pace  
Elliot Anderson  
Koen Laevens  
Mark Birch  
Tom Pietschmann  
Thomas Sjögren  
James Trigg  
Graham Eames  
Ron Colvin  
Simon John  
Ryan Jaynes  
Chad Streck  
Robert McSulla  
Marcus Burghardt  
Matthew Burkett  
Agustin Gonzalez  
Tamas Tevesz

### **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.

DRAFT

## 1.1 Filesystem

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

DRAFT

### 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

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

If available in ANY installed kernel:

- Create a file 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	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

## MITRE ATT&CK Mappings:

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

### **1.1.1.2 Ensure 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_mtype="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/$l_mtype"
    l_mpname=$(tr '-' '_' <<< "$l_mname")
    l_mndir=$(tr '-' '/' <<< "$l_mname")
    module_loadable_chk()
    {
        # Check if the module is currently loadable
        l_loadable=$(modprobe -n -v "$l_mname")
        [ "$?" -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_mtype" ]; 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 with `install freevxfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file with `blacklist freevxfs` in the `/etc/modprobe.d/` directory
- Unload `freevxfs` from the kernel

If available in ANY installed kernel:

- Create a file 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	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

## MITRE ATT&CK Mappings:

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

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

If available in ANY installed kernel:

- Create a file 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	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

## MITRE ATT&CK Mappings:

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

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

If available in ANY installed kernel:

- Create a file 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	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

## MITRE ATT&CK Mappings:

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

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

If available in ANY installed kernel:

- Create a file 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	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

## MITRE ATT&CK Mappings:

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

### **1.1.1.6 Ensure overlayfs kernel module is not available (Automated)**

#### **Profile Applicability:**

- Level 1 – Server
- Level 1 – Workstation

#### **Description:**

The `overlayfs` (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 `overlayfs` 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="overlayfs" # 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 `overlayfs` module:  
If the module is available in the running kernel:

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

If available in ANY installed kernel:

- Create a file with `blacklist overlayfs` 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="overlayfs" # 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. <https://docs.kernel.org/filesystems/overlayfs.html>
2. 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
T1005, T1005.000	TA0005	M1050

### **1.1.1.7 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 utilizes `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 with `install squashfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file with `blacklist squashfs` in the `/etc/modprobe.d/` directory
- Unload `squashfs` from the kernel

If available in ANY installed kernel:

- Create a file 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	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

## MITRE ATT&CK Mappings:

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

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

If available in ANY installed kernel:

- Create a file 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	<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
T1005, T1005.000	TA0005	M1050

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

#### **Profile Applicability:**

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

#### **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 with `install usb-storage /bin/false` in the `/etc/modprobe.d/` directory
- Create a file 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 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
2. NIST SP 800-53 Revision 4 :: IA-3

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-251505  
Rule ID: SV-251505r853450\_rule  
STIG ID: UBTU-20-010461  
Severity: CAT II

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>10.3 Disable Autorun and Autoplay for Removable Media</b> Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	<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.		●	●

## MITRE ATT&CK Mappings:

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

### *1.1.1.10 Ensure data-at-rest encryption is enabled (Manual)*

#### **Profile Applicability:**

- STIG

#### **Description:**

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

#### **Rationale:**

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

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

#### **Audit:**

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

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

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

```
# fdisk -l

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

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

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

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

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

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

## **Remediation:**

To encrypt an entire partition, dedicate a partition for encryption in the partition layout.  
**Note:** Encrypting a partition in an already-installed system is more difficult because it will need to be resized and existing partitions changed.

## **References:**

1. NIST SP 800-53 Revision 5 :: SC-28 (1)
2. NIST SP 800-53 Revision 4 :: SC-28 (1)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238335  
Rule ID: SV-238335r654180\_rule  
STIG ID: UBTU-20-010414  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>14.8 Encrypt Sensitive Information at Rest</b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

### *1.1.1.11 Ensure data-at-rest employs cryptographic mechanisms to prevent unauthorized modification (Manual)*

#### **Profile Applicability:**

- STIG

#### **Description:**

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

#### **Rationale:**

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

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

#### **Audit:**

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

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

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

```
# fdisk -l

(...)

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

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

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

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

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

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

## **Remediation:**

To encrypt an entire partition, dedicate a partition for encryption in the partition layout.  
**Note:** Encrypting a partition in an already-installed system is more difficult because it will need to be resized and existing partitions changed.

## **References:**

1. NIST SP 800-53 Revision 5 :: SC-28 (1)
2. NIST SP 800-53 Revision 4 :: SC-28 (1)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238365  
Rule ID: SV-238365r654270\_rule  
STIG ID: UBTU-20-010444  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>14.8 Encrypt Sensitive Information at Rest</b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

## *1.1.1.12 Ensure sticky bit is set on all world-writable directories (Automated)*

### **Profile Applicability:**

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

### **Description:**

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

### **Rationale:**

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

### **Audit:**

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

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

No output should be returned.

### **Remediation:**

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

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

### **References:**

1. NIST SP 800-53 Revision 5 :: SC-4

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238332  
Rule ID: SV-238332r654171\_rule  
STIG ID: UBTU-20-010411  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

## 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:**

- 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
- 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 /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.

DRAFT

### *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 -nk /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`.

##### **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)

DRAFT

### *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 could be mounted anywhere and are not necessarily restricted to `/home`, nor restricted to a single location, nor is the name restricted in any way.

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

DRAFT

### *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 reasoning for mounting `/home` on a separate partition is as follows.

##### **Protection from resource exhaustion**

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

##### **Fine grained control over the mount**

Configuring `/home` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options 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.

##### **Protection of user data**

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

#### **Impact:**

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

#### **Audit:**

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

```
# findmnt -nk /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/>

## **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 -nk /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 -nk /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.

DRAFT

#### *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.

###### **Protection from resource exhaustion**

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

###### **Fine grained control over the mount**

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

###### **Protection from exploitation**

An example of exploiting `/var` may be an attacker establishing a hard-link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard-link would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

##### **Impact:**

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

## Audit:

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

Example:

```
# findmnt -nk /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/>

## 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:**

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

DRAFT

#### *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 -nk /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 -nk /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.

DRAFT

### **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 reasoning for mounting `/var/tmp` on a separate partition is as follows.

##### **Protection from resource exhaustion**

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

##### **Fine grained control over the mount**

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

##### **Protection from exploitation**

An example of exploiting `/var/tmp` may be an attacker establishing a hard-link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard-link would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

#### **Impact:**

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

## Audit:

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

```
# findmnt -nk /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/>

## 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

DRAFT

## **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 -nk /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 -nk /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 -nk /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  
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.

DRAFT

### *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 reasoning for mounting `/var/log` on a separate partition is as follows.

##### **Protection from resource exhaustion**

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 as a whole.

##### **Fine grained control over the mount**

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

##### **Protection of log data**

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

#### **Impact:**

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

## Audit:

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

```
# findmnt -nk /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/>

## 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 -nk /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 -nk /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 -nk /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  
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.

DRAFT

### **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 reasoning for mounting `/var/log/audit` on a separate partition is as follows.

#### **Protection from resource exhaustion**

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.

#### **Fine grained control over the mount**

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

#### **Protection of audit data**

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

#### **Impact:**

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

## Audit:

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

```
# findmnt -nk /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/>

## 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 -nk /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 -nk /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.

## 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 -nk /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.

## 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 Configure Software and Patch Management

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 reveal the patched exploitable entry points to the public. Public knowledge of these exploits cans 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

DRAFT

### *1.2.1 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 -s upgrade
```

#### **Remediation:**

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

```
# apt upgrade
```

**OR**

```
# apt dist-upgrade
```

#### **References:**

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

## **Additional Information:**

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

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

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●
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:**

Techniques / Sub-techniques	Tactics	Mitigations
T1211, T1211.000	TA0004, TA0008	M1051

DRAFT

## *1.2.2 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>	●	●	●
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
T1068, T1068.000, T1195, T1195.001, T1195.002, T1203, T1203.000, T1210, T1210.000, T1211, T1211.000, T1212, T1212.000	TA0001	M1051

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

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify GPG keys are configured correctly for your package manager:

```
# apt-key list
```

#### **Remediation:**

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

#### **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>	●	●	●
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

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

### **Profile Applicability:**

- STIG

### **Description:**

The operating system's Advance Package Tool (APT) must be configured to prevent the installation of patches, service packs, device drivers, or operating system components without verification they have been digitally signed using a certificate that is recognized and approved by the organization.

### **Rationale:**

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

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

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

### **Audit:**

Verify that APT is configured to prevent the installation of patches, service packs, device drivers, or operating system components without verification they have been digitally signed using a certificate that is recognized and approved by the organization. Check that the "AllowUnauthenticated" variable is not set at all or is set to "false" with the following command:

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

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

## **Remediation:**

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

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

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

## **References:**

1. NIST SP 800-53 Revision 4 :: CM-5 (3)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238359  
Rule ID: SV-238359r654319\_rule  
STIG ID: UBTU-20-010438  
Severity: CAT II

## **CIS Controls:**

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

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

### **Profile Applicability:**

- STIG

### **Description:**

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

### **Rationale:**

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

### **Audit:**

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

```
# grep -i remove-unused /etc/apt/apt.conf.d/50unattended-upgrades
```

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

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

### **Remediation:**

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

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

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

### **References:**

1. NIST SP 800-53 Revision 5 :: SI-2 (6)
2. NIST SP 800-53 Revision 4 :: SI-2 (6)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238370  
Rule ID: SV-238370r654285\_rule  
STIG ID: UBTU-20-010449  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●
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.	●	●	●

### **1.3 Secure Boot Settings**

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

DRAFT

### *1.3.1 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>
# grep "^password" /boot/grub/grub.cfg
password_pbkdf2 <username> <encrypted-password>
```

## **Remediation:**

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

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

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

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

*The superuser/user information and password should not be contained in the `/etc/grub.d/00_header` file as this file could be overwritten in a package update. If there is a requirement to be able to boot/reboot without entering the password, edit `/etc/grub.d/10_linux` and add --unrestricted to the line CLASS=*

*Example:*

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

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

```
# update-grub
```

## **Default Value:**

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

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

## **References:**

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

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide Version 1, Release: 9 Benchmark Date: 26 Jul 2023
Vul ID: V-238204
Rule ID: SV-238204r832936_rule
STIG ID: UBTU-20-010009
Severity: CAT I

## **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
T1542, T1542.000	TA0003	M1046

### *1.3.2 Ensure permissions on bootloader config are configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Run the following command and verify **Uid and Gid are both 0/root and Access is 0600 or more restrictive.**

```
# stat /boot/grub/grub.cfg
Access: (0600/-r-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

#### **Remediation:**

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

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

#### **References:**

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

#### **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	<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	TA0005, TA0007	M1022

### *1.3.3 Ensure authentication required for single user mode (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

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

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

No results should be returned.

#### **Remediation:**

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

```
# passwd root
```

#### **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
T1548, T1548.000	TA0005	M1022

DRAFT

## 1.4 Additional Process Hardening

DRAFT

### *1.4.1 Ensure XD/NX support is enabled (Manual)*

#### **Profile Applicability:**

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

#### **Description:**

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

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

#### **Rationale:**

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

#### **Audit:**

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

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

**- OR -**

on systems without journalctl:

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

Nothing should be returned

## **Remediation:**

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

If necessary configure your bootloader to load the new kernel and reboot the system. You may need to enable NX or XD support in your bios.

## **References:**

1. NIST SP 800-53 Revision 5 :: SI-16
2. NIST SP 800-53 Revision 4 :: SI-16

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238368

Rule ID: SV-238368r654279\_rule

STIG ID: UBTU-20-010447

Severity: CAT II

## **CIS Controls:**

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

## *1.4.2 Ensure address space layout randomization (ASLR) is enabled (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process.

### **Rationale:**

Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

### **Audit:**

Run the following 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 conically 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 "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
    fi
}

```

## **Remediation:**

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

- `kernel.randomize_va_space = 2`

### *Example:*

```
# printf "\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 conically 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:**

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

DRAFT

### *1.4.3 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 conically 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_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`:

- `kernel.yama.ptrace_scope = 1`

### *Example:*

```
# printf "\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 conically later file, or later in the same file, these settings will be overwritten

### **Default Value:**

`kernel.yama.ptrace_scope=1`

### **References:**

1. <https://www.kernel.org/doc/Documentation/security/Yama.txt>
2. <https://github.com/raj3shp/termspy>

### **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:**

Techniques / Sub-techniques	Tactics	Mitigations
T1055.008		

DRAFT

#### *1.4.4 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 -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
prelink  
  
prelink      unknown  ok  not-installed          not-installed
```

##### **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

## *1.4.5 Ensure maxlogins is 10 or less (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

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

### **Rationale:**

The operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based upon mission needs and the operational environment for each system.

### **Audit:**

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

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

The result must contain the following line:

- hard maxlogins 10

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

### **Remediation:**

Configure the operating system to limit the number of concurrent sessions to 10 for all accounts and/or account types.

Add the following line to the top of the `/etc/security/limits.conf` file:

```
* hard maxlogins 10
```

### **References:**

1. NIST SP 800-53 Revision 5 :: AC-10

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238323  
Rule ID: SV-238323r654144\_rule  
STIG ID: UBTU-20-010400  
Severity: CAT III

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

## *1.4.6 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 2>&1 && 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 disable the apport service

```
# systemctl stop apport.service  
# systemctl --now disable 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>		●	●

## *1.4.7 Ensure kdump service is not enabled (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

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

### **Rationale:**

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system partition.

### **Audit:**

Verify that kernel core dumps are disabled unless needed.

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

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

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

If the service is active and is not documented, this is a finding.

### **Remediation:**

If kernel core dumps are not required, disable the "kdump" service with the following command:

```
# systemctl disable kdump.service
```

If kernel core dumps are required, document the need with the ISSO.

### **References:**

1. NIST SP 800-53 Revision 5 :: SC-24

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238334

Rule ID: SV-238334r654177\_rule

STIG ID: UBTU-20-010413

Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.		●	●

## *1.4.8 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 -Es '^(\*|\s).*hard.*core.*(\s+\#.*)?$' /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 conically 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]+\.[^\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 is-enabled coredump.service
```

if enabled, masked, or disabled is returned systemd-coredump is installed

### Remediation:

Add the following line to /etc/security/limits.conf or a /etc/security/limits.d/\* file:

```
* hard core 0
```

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

- fs.suid\_dumpable = 0

### Example:

```
# printf "  
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 conically 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
```

### MITRE ATT&CK Mappings:

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

## **1.4.9 Ensure the Ctrl-Alt-Delete key sequence is disabled (Automated)**

### **Profile Applicability:**

- STIG

### **Description:**

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

### **Rationale:**

A locally logged-on user who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot.

### **Audit:**

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

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

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

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

### **Remediation:**

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

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

Reload the daemon to take effect:

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

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238380  
Rule ID: SV-238380r654315\_rule  
STIG ID: UBTU-20-010460  
Severity: CAT I

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

#### *1.4.10 Ensure dmesg\_restrict is enabled (Automated)*

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

- STIG

##### **Description:**

The `kernel.dmesg_restrict` kernel parameter can be used to configure the Linux kernel and restrict access to information from dmesg.

##### **Rationale:**

Restricting access to the kernel message buffer limits access only to root. This prevents attackers from gaining additional system information as a nonprivileged 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.dmesg_restrict 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 conically 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.dmesg_restrict=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`:

- `kernel.dmesg_restrict = 1`

### **Example:**

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

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.dmesg_restrict=1
```

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

### **Default Value:**

`kernel.dmesg_restrict=1`

### **References:**

1. NIST SP 800-53 :: SC-4

### **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-255913  
Rule ID: SV-255913r880908\_rule  
STIG ID: UBTU-20-010401  
Severity: CAT III

### **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
T1055.008		

DRAFT

## 1.5 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.

**Note:**

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

### 1.5.1 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/>

### 1.5.1.1 Ensure AppArmor is installed (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

AppArmor provides Mandatory Access Controls.

#### Rationale:

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

#### Audit:

Verify that AppArmor is installed:

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
apparmor apparmor-utils  
  
apparmor      install ok installed      installed  
apparmor-utils  install ok installed      installed
```

#### Remediation:

Install AppArmor.

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

#### 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>
T1068, T1068.000, T1565, T1565.001, T1565.003	TA0003	M1026

DRAFT

### *1.5.1.2 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

### *1.5.1.3 Ensure AppArmor is installed, enabled, and active (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The Ubuntu operating system must be configured to use AppArmor.

#### **Rationale:**

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

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

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

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

#### **Audit:**

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

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

```
# dpkg -l | grep apparmor
```

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

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

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

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

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

## **Remediation:**

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

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

Start "apparmor" with the following command:

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

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

## **References:**

1. NIST SP 800-53 Revision 5 :: CM-7 (2)
2. NIST SP 800-53 Revision 5 :: CM-7 (5) (b)
3. NIST SP 800-53 Revision 5 :: AC-3 (4)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238360  
Rule ID: SV-238360r654255\_rule  
STIG ID: UBTU-20-010439  
Severity: CAT II

## **CIS Controls:**

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

#### *1.5.1.4 Ensure all AppArmor Profiles are in enforce or complain mode (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

AppArmor profiles define what resources applications are able to access.

##### **Rationale:**

Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that any policies that exist on the system are activated.

##### **Audit:**

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

```
# apparmor_status | grep profiles
```

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

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

Run the following command and verify no processes are unconfined

```
# apparmor_status | grep processes
```

Review the output and ensure no processes are unconfined:

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

## **Remediation:**

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

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

-- OR --

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

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

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

## **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
	TA0005	

### *1.5.1.5 Ensure all AppArmor Profiles are enforcing (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

AppArmor profiles define what resources applications are able to access.

#### **Rationale:**

Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that any policies that exist on the system are activated.

#### **Audit:**

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

```
# apparmor_status | grep profiles
```

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

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

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

```
apparmor_status | grep processes
```

Review the output and ensure no processes are unconfined:

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

#### **Remediation:**

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

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

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

#### **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	

## 1.6 Command Line Warning Banners

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

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

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

## *1.6.1 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 no results are returned:

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

## **Remediation:**

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

*Example Text:*

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

-- 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-3

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

Techniques / Sub-techniques	Tactics	Mitigations
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. Add or update the message text to follow local site policy.

*Example Text:*

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

## **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. Add or update the message text to follow local site policy.

*Example Text:*

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

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

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

## *1.6.4 Ensure permissions on /etc/motd are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

### **Rationale:**

If the `/etc/motd` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

### **Audit:**

Run the following command and verify 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 permissions on `/etc/motd`:

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

-- OR --

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

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

### **Default Value:**

File doesn't exist

### **Additional Information:**

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

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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 permissions on /etc/issue are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

### **Rationale:**

If the `/etc/issue` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

### **Audit:**

Run the following command and verify 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 permissions on `/etc/issue`:

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

### **Default Value:**

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

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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 permissions on /etc/issue.net are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

### **Rationale:**

If the `/etc/issue.net` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

### **Audit:**

Run the following command and verify 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 permissions on `/etc/issue.net`:

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

### **Default Value:**

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

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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 GNOME Display Manager

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

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

DRAFT

### *1.7.1 Ensure GNOME Display Manager is removed (Automated)*

#### **Profile Applicability:**

- Level 2 - Server

#### **Description:**

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

#### **Rationale:**

If a Graphical User Interface (GUI) is not required, it should be removed to reduce the attack surface of the system.

#### **Impact:**

Removing the GNOME Display manager will remove the Graphical User Interface (GUI) from the system.

#### **Audit:**

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n' gdm3
gdm3      unknown  ok  not-installed          not-installed
```

#### **Remediation:**

Run the following command to uninstall `gdm3`:

```
# apt purge 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	

### *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:**

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

```

#!/usr/bin/env bash

{
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pk in $l_pcl; do
        $l_pq "$l_pk" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pk\" exists
on the system\n - checking configuration"
    done
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        echo -e "$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
}

```

## Remediation:

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

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

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

        l_gdmprofile="gdm" # Set this to desired profile name IaW Local site policy
        l_bmessage="Authorized uses only. All activity may be monitored and reported"
        # Set to desired banner message
        if [ ! -f "/etc/dconf/profile/$l_gdmprofile" ]; then
            echo "Creating profile \"$l_gdmprofile\""
            echo -e "user-db:user\nsystem-db:$l_gdmprofile\nfile-
db:/usr/share/$l_gdmprofile/greeter-dconf-defaults" > /etc/dconf/profile/$l_gdmprofile
        fi
        if [ ! -d "/etc/dconf/db/$l_gdmprofile.d/" ]; then
            echo "Creating dconf database directory \"/etc/dconf/db/$l_gdmprofile.d/"
            mkdir /etc/dconf/db/$l_gdmprofile.d/
        fi
        if ! grep -Piq '^h*banner-message-enable|h*=\\h*true\\b'
        /etc/dconf/db/$l_gdmprofile.d/*; then
            echo "creating gdm keyfile for machine-wide settings"
            if ! grep -Piq - '^h*banner-message-enable|h*' \
        /etc/dconf/db/$l_gdmprofile.d/*; then
                l_kfile="/etc/dconf/db/$l_gdmprofile.d/01-banner-message"
                echo -e "\n[org/gnome/login-screen]\nbanner-message-enable=true" >>
"$l_kfile"
            else
                l_kfile="$(grep -Pil - '^h*banner-message-enable|h*' \
        /etc/dconf/db/$l_gdmprofile.d/*)"
                ! grep -Pq '^h*[\\org\\/gnome\\/login-screen]\\]' "$l_kfile" && sed -ri
'/^s*banner-message-enable/ i[\\org\\/gnome\\/login-screen]' "$l_kfile"
                ! grep -Pq '^h*banner-message-enable|h*=\\h*true\\b' "$l_kfile" && sed -ri
's/^s*(banner-message-enable\\s*=\\s*)(\\S+)(\\s*.*)/\\1true \\3//' "$l_kfile"
                #           sed -ri '/^s*[\\org\\/gnome\\/login-screen]/ a\\nbanner-message-
enable=true' "$l_kfile"
            fi
        fi
        if ! grep -Piq "^h*banner-message-text=[\\'\\"]+\$+" "$l_kfile"; then
            sed -ri "/^s*banner-message-enable/ a\\nbanner-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
}
```

**Note:**

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

Run the following command to remove the gdm3 package:

```
# apt purge gdm3
```

**Default Value:**

disabled

**References:**

1. <https://help.gnome.org/admin/system-admin-guide/stable/login-banner.html.en>
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
	TA0007	

### *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:**

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

```

#!/usr/bin/env bash

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

```

## **Remediation:**

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

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

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

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

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

**OR**

Run the following command to remove the GNOME package:

```
# apt purge gdm3
```

## **Default Value:**

false

## **References:**

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

### **Description:**

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

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

### *Example key file:*

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

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

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

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

### **Rationale:**

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

### **Audit:**

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

```

#!/usr/bin/env bash

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

```

```

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

```

**Note:**

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

## Remediation:

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

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

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

*Example:*

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

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

*Example:*

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

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

*Example script:*

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

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

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

Run the following command to update the system databases:

```
# dconf update
```

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

## References:

1. <https://help.gnome.org/admin/system-admin-guide/stable/desktop-lockscreen.html.en>
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5
3. NIST SP 800-53 :: AC-11 b
4. NIST SP 800-53 :: AC-11 a

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238199  
Rule ID: SV-238199r653772\_rule  
STIG ID: UBTU-20-010004  
Severity: CAT II

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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
T1461	TA0027	

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

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

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

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

### *Example Lock File:*

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

### **Rationale:**

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

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

## Audit:

Run the following script to verify that the screen lock 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 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
        done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        # Look for idle-delay to determine profile in use, needed for remaining tests
        l_kfd="/etc/dconf/db/${(grep -Psrl '^\h*idle-delay\h*=\'\h*uint32\h+\d+\b' /etc/dconf/db/*) | awk -F'/' '{split(${NF-1},a,".");print a[1]}').d" #set directory of key file to be locked
        l_kfd2="/etc/dconf/db/${(grep -Psrl '^\h*lock-delay\h*=\'\h*uint32\h+\d+\b' /etc/dconf/db/*) | awk -F'/' '{split(${NF-1},a,".");print a[1]}').d" #set directory of key file to be locked
        if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked
            if grep -Prilq '/org/gnome/desktop/session/idle-delay\b' "$l_kfd"; then
                l_output="$l_output\n - \"idle-delay\" is locked in \"$(grep -Pril
'org/gnome/desktop/session/idle-delay\b' "$l_kfd")\""
            else
                l_output2="$l_output2\n - \"idle-delay\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"idle-delay\" is not set so it can not be locked"
        fi
        if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist, options can't be locked
            if grep -Prilq '/org/gnome/desktop/screensaver/lock-delay\b' "$l_kfd2"; then
                l_output="$l_output\n - \"lock-delay\" is locked in \"$(grep -Pril
'org/gnome/desktop/screensaver/lock-delay\b' "$l_kfd2")\""
            else
                l_output2="$l_output2\n - \"lock-delay\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"lock-delay\" is not set so it can not be locked"
        fi
    else
        l_output="$l_output\n - GNOME Desktop Manager package is not installed on the system\n -
Recommendation is not applicable"
    fi
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_pkgoutput" ] && echo -e "\n$l_pkgoutput"
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
    fi
}
```

**Remediation:**

Run the following script to ensure screen locks cannot be overridden:

DRAFT

```

#!/usr/bin/env bash

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

```

Run the following command to update the system databases:

```
# dconf update
```

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

### References:

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

## *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:**

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 -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$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="$l_output\n - dconf database profile isn't set"
            fi
            # Check if the dconf database file exists
            if [ -f "/etc/dconf/db/$l_gpname" ]; then
                l_output="$l_output\n - The dconf database \"$l_gpname\" exists"
            else
                l_output2="$l_output\n - The dconf database \"$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_output\n - The dconf directory \"$l_gpdir\" doesn't exist"
            fi
            # check automount setting
            if grep -PqrS -- '^h*automount\b*=h*false\b' "$l_kfile"; then
                l_output="$l_output\n - \"automount\" is set to false in: \"$l_kfile\""
            else
                l_output2="$l_output\n - \"automount\" is not set correctly"
            fi
            # check automount-open setting
            if grep -Pqs -- '^h*automount-open\b*=h*false\b' "$l_kfile2"; then
                l_output="$l_output\n - \"automount-open\" is set to false in: \"$l_kfile2\""
            else
                l_output2="$l_output\n - \"automount-open\" is not set correctly"
            fi
        else
            # Setings don't exist. Nothing further to check
            l_output2="$l_output\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
}

```

```
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
}
```

DRAFT

**Remediation:**

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

DRAFT

```

#!/usr/bin/env bash

{
    l_pkgoutput="" l_output="" l_output2=""
    l_gpname="local" # Set to desired dconf profile name (defaule 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 -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
    done
    echo -e "$l_packageout"
    # Check configuration (If applicable)
    if [ -n "$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:$l_gpname\b' /etc/dconf/profile/*)\""
        else
            [ ! -f "/etc/dconf/profile/user" ] && l_gpfile="/etc/dconf/profile/user" ||
            l_gpfile="/etc/dconf/profile/user2"
            echo -e " - creating dconf database profile"
            {
                echo -e "\nuser-db:user"
                echo "system-db:$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 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\""
        fi
    done
}

```

```

! grep -Psq -- '\^h*[org]/desktop/media-handling]\b' "$l_kfile" && echo
'[org/gnome/desktop/media-handling]' >> "$l_kfile"
    sed -ri '/^\s*[org]/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]/desktop/media-handling]\b' "$l_kfile" && echo
'[org/gnome/desktop/media-handling]' >> "$l_kfile"
    sed -ri '/^\s*[org]/desktop/media-handling]\b/a \\nautomount=false' "$l_kfile"
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
}

```

## OR

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

```
# apt purge gdm3
```

### 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	<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	TA0008	M1042

DRAFT

## *1.7.7 Ensure user's session lock is enabled (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

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

### **Rationale:**

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

### **Audit:**

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

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

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

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

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

### **Remediation:**

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

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

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

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

### **References:**

1. NIST SP 800-53 Revision 5 :: AC-11 b
2. NIST SP 800-53 Revision 5 :: AC-11 a

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023  
Vul ID: V-238199  
Rule ID: SV-238199r653772\_rule  
STIG ID: UBTU-20-010004  
Severity: CAT II

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●

## *1.7.8 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.

### *Example Lock File:*

```
# Lock desktop screensaver settings  
/org/gnome/desktop/media-handling/automount  
/org/gnome/desktop/media-handling/automount-open
```

### **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 disable automatic mounting is locked:

```

#!/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 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        # Look for idle-delay to determine profile in use, needed for remaining tests
        l_kfd="/etc/dconf/db/$(grep -Psrl '^h*automount\b' /etc/dconf/db/* | awk -F'/
'{split($NF-1,a,".");print a[1]}').d" #set directory of key file to be locked
        l_kfd2="/etc/dconf/db/$(grep -Psrl '^h*automount-open\b' /etc/dconf/db/* | awk -F'/
'{split($NF-1,a,".");print a[1]}').d" #set directory of key file to be locked
        if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked
            if grep -Piq '^h*/org/gnome/desktop/media-handling/automount\b' "$l_kfd"; then
                l_output="$l_output\n - \"automount\" is locked in \"$(grep -Pil
'^h*/org/gnome/desktop/media-handling/automount\b' \"$l_kfd\")\""
            else
                l_output2="$l_output2\n - \"automount\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"automount\" is not set so it can not be locked"
        fi
        if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist, options can't be locked
            if grep -Piq '^h*/org/gnome/desktop/media-handling/automount-open\b' "$l_kfd2";
then
                l_output="$l_output\n - \"lautomount-open\" is locked in \"$(grep -Pril
'^h*/org/gnome/desktop/media-handling/automount-open\b' \"$l_kfd2\")\""
            else
                l_output2="$l_output2\n - \"automount-open\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"automount-open\" is not set so it can not be locked"
        fi
    else
        l_output="$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:\n$l_output\n"
    fi
}

```

Remediation:

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

DRAFT

```

#!/usr/bin/env bash

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

```

**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

**MITRE ATT&CK Mappings:**

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

### *1.7.9 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:**

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 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package:
\"$l_pn\" 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 -Prls -- '^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 "$l_gpname" ]; then
            l_gmdir="/etc/dconf/db/$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 "$l_gmdir" ]; then
                l_output="$l_output\n - The dconf directory \"$l_gmdir\" exitst"
            else
                l_output2="$l_output2\n - The dconf directory \"$l_gmdir\" doesn't exist"
            fi
            # check autorun-never setting
            if grep -Pqrs -- '^\h*autorun-never\h*=\h*true\b' "$l_kfile"; then
                l_output="$l_output\n - \"autorun-never\" is set to true in: \"$l_kfile\""
            else
                l_output2="$l_output2\n - \"autorun-never\" is not set correctly"
            fi
        else
            # Settings don't exist. Nothing further to check
            l_output2="$l_output2\n - \"autorun-never\" is not set"
        fi
    else
        l_output="$l_output\n - GNOME Desktop Manager package is not installed on the
        system\n - Recommendation is not applicable"
    fi
}

```

```
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
}
```

DRAFT

**Remediation:**

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

DRAFT

```

#!/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 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package:
\"$l_pn\" 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 -Prls -- '^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_gmdir="/etc/dconf/db/$l_gpname.d"
        if [ -d "$l_gmdir" ]; then
            echo " - The dconf database directory \"$l_gmdir\" exists"
        else
            echo " - creating dconf database directory \"$l_gmdir\""
            mkdir "$l_gmdir"
        fi
        # check autorun-never setting
        if grep -Pqs -- '^h*autorun-never\h*=\h*true\b' "$l_kfile"; then
            echo " - \"autorun-never\" is set to true in: \"$l_kfile\""
        else
            echo " - creating or updating \"autorun-never\" entry in \"$l_kfile\""
            if grep -Psq -- '^h*autorun-never' "$l_kfile"; then
                sed -ri 's/(^s*autorun-never\s*=\s*)(\S+)(\s.*$)/\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 -\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

## *1.7.10 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.

Example Lock File:

```
# Lock desktop media-handling settings  
/org/gnome/desktop/media-handling/autorun-never
```

### **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 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
    Package: \"$l_pn\" exists on the system\n - checking configuration"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        # Look for idle-delay to determine profile in use, needed for remaining
        tests
        l_kfd="/etc/dconf/db/$(grep -Psril '^h*autorun-never\b' \
/etc/dconf/db/* | awk -F'/' '{split(${NF-1},a,".");print a[1]}').d" #set
        directory of key file to be locked
        if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options
        can't be locked
            if grep -Prisq '^h*/org/gnome/desktop/media-handling/autorun-
        never\b' "$l_kfd"; then
                l_output="$l_output\n - \"autorun-never\" is locked in \"$(grep -
        Pril '^h*/org/gnome/desktop/media-handling/autorun-never\b' "$l_kfd")\""
            else
                l_output2="$l_output2\n - \"autorun-never\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"autorun-never\" is not set so it can not
        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 "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
    fi
}

```

## **Remediation:**

Run the following script to ensure 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 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_dn in $l_pcl; do
        $l_pq "$l_dn" > /dev/null 2>&1 && l_pkgoutput="y" && echo -e "\n - Package: \"$l_dn\"\n
exists on the system\n - remediating configuration if needed"
        done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        # Look for autorun to determine profile in use, needed for remaining tests
        l_kfd="/etc/dconf/db/${(grep -Psril '^h*autorun-never\b' /etc/dconf/db/*/ | awk -F'/'\'
        '{split(${NF-1},a,".");print a[1]}').d}" #set directory of key file to be locked
        if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked
            if grep -Prisq '^h*/org/gnome/desktop/media-handling/autorun-never\b' "$l_kfd";
        then
            echo " - \"autorun-never\" is locked in \"$(grep -Pril
            '^h*/org/gnome/desktop/media-handling/autorun-never\b' "$l_kfd")\""
            else
                echo " - creating entry to lock \"autorun-never\""
                [ ! -d "$l_kfd"/locks ] && echo "creating directory $l_kfd/locks" && mkdir
        "$l_kfd"/locks
            {
                echo -e '\n# Lock desktop media-handling autorun-never setting'
                echo '/org/gnome/desktop/media-handling/autorun-never'
            } >> "$l_kfd"/locks/00-media-autorun
        fi
    else
        echo -e " - \"autorun-never\" is not set so it can not be locked\n - Please follow
        Recommendation \"Ensure GDM autorun-never is enabled\" and follow this Recommendation again"
        fi
        # update dconf database
        dconf update
    else
        echo -e " - GNOME Desktop Manager package is not installed on the system\n -
        Recommendation is not applicable"
        fi
    }
}
```

## **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	10.3 <u>Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 <u>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	M1028

### *1.7.11 Ensure XDCMP is not enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

X Display Manager Control Protocol (XDMCP) is designed to provide authenticated access to display management services for remote displays

#### **Rationale:**

XDMCP is inherently insecure.

- XDMCP is not a ciphered protocol. This may allow an attacker to capture keystrokes entered by a user
- XDMCP is vulnerable to man-in-the-middle attacks. This may allow an attacker to steal the credentials of legitimate users by impersonating the XDMCP server.

#### **Audit:**

Run the following command and verify the output:

```
# grep -Eis '^s*Enable\s*=\s*true' /etc/gdm3/custom.conf  
Nothing should be returned
```

#### **Remediation:**

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

```
Enable=true
```

#### **Default Value:**

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

#### **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

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

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local access to the system via a graphical user logon.

#### **Rationale:**

Display of a standardized and approved use notification before granting access to the Ubuntu operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

## Audit:

Verify the Ubuntu operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon.

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

Verify the operating system displays the exact approved Standard Mandatory DoD Notice and Consent Banner text with the command:

```
# grep ^banner-message-text /etc/gdm3/greeter.dconf-defaults
```

Output should read:

```
banner-message-text="You are accessing a U.S. Government \USG\ Information System \IS\ that is provided for USG-authorized use only.\s+By using this IS \which includes any device attached to this IS\, you consent to the following conditions:\s+-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct \PM\, law enforcement \LE\, and counterintelligence \CI\ investigations.\s+-At any time, the USG may inspect and seize data stored on this IS.\s+-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.\s+-This IS includes security measures \e.g., authentication and access controls\ to protect USG interests--not for your personal benefit or privacy.\s+-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."
```

If the banner-message-text is missing, commented out, or does not match the Standard Mandatory DoD Notice and Consent Banner exactly, this is a finding.

## **Remediation:**

Edit the "/etc/gdm3/greeter.dconf-defaults" file.

Set the "banner-message-text" line to contain the appropriate banner message text as shown below:

```
banner-message-text='You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.\n\nBy using this IS (which includes any device attached to this IS), you consent to the following conditions:\n\n-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.\n\n-At any time, the USG may inspect and seize data stored on this IS.\n\n-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.\n\n-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.\n\n-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.'
```

Update the GDM with the new configuration:

```
# dconf update
# systemctl restart gdm3
```

## **References:**

1. NIST SP 800-53 Rev. 5: AC-8 a

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238197, V-238198  
Rule ID: SV-238197r653766\_rule  
STIG ID: UBTU-20-010002  
Severity: CAT II  
Vul ID: V-238198  
Rule ID: SV-238198r653769\_rule  
STIG ID: UBTU-20-010003  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

### *1.7.13 Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must disable the x86 Ctrl-Alt-Delete key sequence if a graphical user interface is installed.

#### **Rationale:**

A locally logged-on user who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In the graphical environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

#### **Audit:**

Verify the Ubuntu operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface.

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

```
# grep logout /etc/dconf/db/local.d/*
logout=''
```

If the "logout" key is bound to an action, is commented out, or is missing, this is a finding.

#### **Remediation:**

Configure the system to disable the Ctrl-Alt-Delete sequence when using a graphical user interface by creating or editing the /etc/dconf/db/local.d/00-disable-CAD file. Add the setting to disable the Ctrl-Alt-Delete sequence for the graphical user interface:

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

Update the dconf settings:

```
# dconf update
```

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238379  
Rule ID: SV-238379r654312\_rule  
STIG ID: UBTU-20-010459  
Severity: CAT I

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

## **1.8 Additional Software**

Install additional software packages

DRAFT

## *1.8.1 Ensure vlock is installed (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must allow users to directly initiate a session lock for all connection types.

### **Rationale:**

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, the Ubuntu operating systems need to provide users with the ability to manually invoke a session lock so users may secure their session if they need to temporarily vacate the immediate physical vicinity.

### **Audit:**

Verify the "vlock" package is installed by running the following command:

```
# dpkg -l | grep vlock
```

If "vlock" is not installed, this is a finding.

### **Remediation:**

Install the "vlock" package (if it is not already installed) by running the following command:

```
# apt install vlock
```

### **References:**

1. NIST SP 800-53 :: AC-11 a
2. NIST SP 800-53 :: AC-11 (1)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238200  
Rule ID: SV-238200r653775\_rule  
STIG ID: UBTU-20-010005  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●

## *1.8.2 Ensure Endpoint Security for Linux Threat Prevention is installed (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

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

### **Rationale:**

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

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

### **Audit:**

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

Check that the "mfntp" package has been installed:

```
# dpkg -l | grep mcafeftp
```

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

Check that the daemon is running:

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

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

### **Remediation:**

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

Configure the Ubuntu operating system to use ENSLTP.

Install the "mfntp" package:

```
# apt-get install mcafeftp
```

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238336  
Rule ID: SV-238336r858538\_rule  
STIG ID: UBTU-20-010415  
Severity: CAT III

## **CIS Controls:**

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

## 1.9 Federal Information Processing Standards (FIPS) Cryptographic Modules

**Note:** Debian Linux 11 does not include the FIPS Kernel cryptographic modules required to enable FIPS.

Title: Ensure FIPS mode is enabled

Description:

The operating system must implement NIST FIPS-validated cryptography to protect classified information and for the following: to provision digital signatures, to generate cryptographic hashes, and to protect unclassified information requiring confidentiality and cryptographic protection in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Rationale Statement:

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Default Value

References:

- NIST SP 800-53 Revision 5 :: SC-13 b
- SRG-OS-000396-GPOS-00176, SRG-OS-000478-GPOS-00223
- <https://www.debian.org/doc/manuals/debian-faq/debian-faq.en.pdf>

Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238363  
Rule ID: SV-238363r654320\_rule  
STIG ID: UBTU-20-010442  
Severity: CAT I

## 2 Services

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

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

### 2.1 Configure Time Synchronization

It is recommended that physical systems and virtual guests lacking direct access to the physical host's clock be configured to synchronize their time using a service such as `systemd-timesyncd`, `chrony`, or `ntp`.

**Note:**

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

### **2.1.1 Ensure time synchronization is in use**

It is recommended that physical systems and virtual guests lacking direct access to the physical host's clock be configured to synchronize their time using a service such as `systemd-timesyncd`, `chrony`, or `ntp`.

DRAFT

## *2.1.1.1 Ensure a single time synchronization daemon is in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of servers and having all systems synchronize their clocks to them.

### **Note:**

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

### **Rationale:**

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

### **Audit:**

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

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

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

```

#!/usr/bin/env bash

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

```

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

## **Remediation:**

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

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

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

1.

`chrony`

Run the following command to install `chrony`:

```
# apt install chrony
```

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

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

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

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

```
# apt purge ntp
```

### **NOTE:**

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

2.

`systemd-timesyncd`

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

```
# apt purge chrony
```

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

```
# apt purge ntp
```

### **NOTE:**

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

3.

`ntp`

Run the following command to install `ntp`:

```
# apt install ntp
```

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

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

Run the following command to remove the chrony package:

```
# apt purge chrony
```

**NOTE:**

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

**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	

## 2.1.2 Configure chrony

chrony is a daemon which implements the Network Time Protocol (NTP) and is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate.

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

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

**Note:**

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

## *2.1.2.1 Ensure chrony is configured with authorized timeserver (Manual)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

## Audit:

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

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

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

*Output examples:*

*pool directive:*

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

*server directive:*

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

## Remediation:

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

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

*Examples:*

*pool directive:*

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

*server directive:*

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

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

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

**OR**

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

```
# apt purge chrony
```

## References:

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

## 2.1.2.2 Ensure chrony is running as user \_chrony (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

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

### Rationale:

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

### Audit:

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

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

Nothing should be returned

### Remediation:

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

```
user _chrony
```

### OR

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

```
# apt purge chrony
```

### Default Value:

`user _chrony`

### 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

### *2.1.2.3 Ensure chrony is enabled and running (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

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

#### **Audit:**

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

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

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

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

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

## **Remediation:**

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

Run the following command to unmask chrony.service:

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

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

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

**OR**

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

```
# apt purge chrony
```

## **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

### 2.1.3 Configure systemd-timesyncd

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

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

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

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

To disable a configuration file supplied by the vendor, the recommended way is to place a symlink to `/dev/null` in the configuration directory in `/etc/`, with the same filename as the vendor configuration file.

**Note:**

- The recommendations in this section only apply if timesyncd is in use on the system
- The systemd-timesyncd service specifically implements only SNTP.
  - This minimalistic service will set the system clock for large offsets or slowly adjust it for smaller deltas
  - More complex use cases are not covered by systemd-timesyncd
- **If chrony or ntp are used, systemd-timesyncd should be stopped and masked, and this section skipped**
- **One, and only one, time synchronization method should be in use on the system**

DRAFT

### *2.1.3.1 Ensure systemd-timesyncd configured with authorized timeserver (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:

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

```
# grep -Ph '^h*(NTP|FallbackNTP)=\H+' /etc/systemd/timesyncd.conf
```

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

*Example Output:*

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

DRAFT

## **Remediation:**

**Edit** /etc/systemd/timesyncd.conf **and add the NTP= and/or FallbackNTP= lines to the [Time] section:**

**Example:**

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

**Note:** Servers added to these line(s) should follow local site policy. NIST servers are for example.

**Example script:**

The following example script will add the example NIST time servers to /etc/systemd/timesyncd.conf

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

{
    l_ntp_ts="time.nist.gov"
    l_ntp_fb="time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov"
    l_conf_file="/etc/systemd/timesyncd.conf"
    if ! grep -Ph '^h*NTP=\H+' "$l_conf_file"; then
        ! grep -Pqs '^h*[Time]' "$l_conf_file" && echo "[Time]" >> "$l_conf_file"
        echo "NTP=$l_ntp_ts" >> "$l_conf_file"
    fi
    if ! grep -Ph '^h*FallbackNTP=\H+' "$l_conf_file"; then
        ! grep -Pqs '^h*[Time]' "$l_conf_file" && echo "[Time]" >> "$l_conf_file"
        echo "FallbackNTP=$l_ntp_fb" >> "$l_conf_file"
    fi
}
```

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

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

**-OR-**

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

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

## **Default Value:**

#NTP=

#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	<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

## *2.1.3.2 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

## 2.1.4 Configure ntp

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

### Note:

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

## 2.1.4.1 Ensure ntp access control is configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

ntp Access Control Commands:

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

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

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

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

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

One or more of the following flags may be specified:

- `kod` - If this flag is set when an access violation occurs, a kiss-o'-death (KoD) packet is sent. KoD packets are rate limited to no more than one per second. If another KoD packet occurs within one second after the last one, the packet is dropped.
- `limited` - Deny service if the packet spacing violates the lower limits specified in the `discard` command. A history of clients is kept using the monitoring capability of `ntpd`. Thus, monitoring is always active as long as there is a restriction entry with the `limited` flag.
- `lowpriotrap` - Declare traps set by matching hosts to be low priority. The number of traps a server can maintain is limited (the current limit is 3). Traps are usually assigned on a first come, first served basis, with later trap requestors being denied service. This flag modifies the assignment algorithm by allowing low priority traps to be overridden by later requests for normal priority traps.

- `nopeer` - Deny ephemeral peer requests, even if they come from an authenticated source. Note that the ability to use a symmetric key for authentication may be restricted to one or more IPs or subnets via the third field of the `ntp.keys` file. This restriction is not enabled by default, to maintain backward compatibility. Expect `nopeer` to become the default in `ntp-4.4`.
- `nomodify` - Deny `ntpq` and `ntpdc` queries which attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.
- `noquery` - Deny `ntpq` and `ntpdc` queries. Time service is not affected.
- `nopeer` - Deny unauthenticated packets which would result in mobilizing a new association. This includes broadcast and symmetric active packets when a configured association does not exist. It also includes pool associations, so if you want to use servers from a pool directive and also want to use `nopeer` by default, you'll want a `restrict source ...` line as well that does not include the `nopeer` directive.
- `noserve` - Deny all packets except `ntpq` and `ntpdc` queries.
- `notrap` - Decline to provide mode 6 control message trap service to matching hosts. The trap service is a subsystem of the `ntpq` control message protocol which is intended for use by remote event logging programs.
- `notrust` - Deny service unless the packet is cryptographically authenticated.
- `ntpport` - This is actually a match algorithm modifier, rather than a restriction flag. Its presence causes the restriction entry to be matched only if the source port in the packet is the standard NTP UDP port (123). Both `ntpport` and `non-ntpport` may be specified. The `ntpport` is considered more specific and is sorted later in the list.

#### Rationale:

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

## Audit:

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

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

Output should be similar to:

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

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

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

## Remediation:

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

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

**OR**

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

```
# apt purge ntp
```

## Default Value:

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

## References:

1. <http://www.ntp.org/>
2. ntp.conf(5)
3. ntpd(8)
4. 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, T1498, T1498.002, T1562, T1562.001	TA0002	M1022

## **2.1.4.2 Ensure ntp is configured with authorized timeserver (Manual)**

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

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

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

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

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

### **Rationale:**

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

## Audit:

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

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

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

*Output examples:*

*pool mode:*

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

*server mode:*

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

## Remediation:

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

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

*Examples:*

*pool mode:*

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

*server mode:*

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

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

```
# systemctl restart ntp
```

**OR**

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

```
# apt purge ntp
```

## References:

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

## 5. 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, T1498, T1498.002, T1562, T1562.001	TA0002	M1022

### *2.1.4.3 Ensure ntp is running as user ntp (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Note:**

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

#### **Rationale:**

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

#### **Audit:**

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

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

Nothing should be returned

Run the following command to verify the `RUNASUSER=` **is set to `ntp` in `/usr/lib/ntp/ntp-systemd-wrapper`:**

```
# grep -P -- '^h*RUNASUSER=' /usr/lib/ntp/ntp-systemd-wrapper
RUNASUSER=ntp
```

## **Remediation:**

Add or edit the following line in `/usr/lib/ntp/ntp-systemd-wrapper`:

```
RUNASUSER=ntp
```

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

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

**OR**

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

```
# apt purge ntp
```

## **Default Value:**

user ntp

## **References:**

1. <http://www.ntp.org/>
2. 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.		●	●

## *2.1.4.4 Ensure ntp is enabled and running (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

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

### **Audit:**

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

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

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

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

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

### **Remediation:**

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

Run the following command to unmask ntp.service:

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

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

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

**OR**

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

```
# apt purge ntp
```

**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.		●	●

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

### **Profile Applicability:**

- STIG

### **Description:**

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

### **Rationale:**

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network. Organizations should consider setting time periods for different types of systems (e.g., financial, legal, or mission-critical systems).

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

### **Audit:**

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

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

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

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

## **Remediation:**

Configure chrony to synchronize the internal system clocks to the authoritative source when the time difference is greater than one second by doing the following:  
Edit the "/etc/chrony/chrony.conf" file and add:

```
makestep 1 -1
```

Restart the chrony service:

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

## **References:**

1. NIST SP 800-53 Revision 4 :: AU-8 (1) (b)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238357

Rule ID: SV-238357r654246\_rule

STIG ID: UBTU-20-010436

Severity: CAT III

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.		●	●

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

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must, for networked systems, compare internal information system clocks at least every 24 hours with a server which is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, or a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

### **Rationale:**

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

## Audit:

If the system is not networked, this requirement is Not Applicable.  
The system clock must be configured to compare the system clock at least every 24 hours to the authoritative time source.  
Check the value of "maxpoll" in the "/etc/chrony/chrony.conf" file with the following command:

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

If "maxpoll" is not set to "17" or does not exist, this is a finding.  
Verify that the "chrony.conf" file is configured to an authoritative DoD time source by running the following command:

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

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

## Remediation:

If the system is not networked, this requirement is Not Applicable.  
To configure the system clock to compare the system clock at least every 24 hours to the authoritative time source, edit the "/etc/chrony/chrony.conf" file. Add or correct the following lines, by replacing "[source]" in the following line with an authoritative DoD time source:

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

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

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

## References:

1. NIST SP 800-53 Revision 4 :: AU-8 (1) (a)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238356

Rule ID: SV-238356r654317\_rule

STIG ID: UBTU-20-010435

Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.		●	●

## *2.1.7 Ensure system timezone is set to UTC or GMT (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

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

### **Rationale:**

If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis.

Time stamps generated by the operating system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

### **Audit:**

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

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

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

### **Remediation:**

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

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

### **References:**

1. NIST SP 800-53 Revision 5 :: AU-8 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238308  
Rule ID: SV-238308r654099\_rule  
STIG ID: UBTU-20-010230  
Severity: CAT III

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

## 2.2 Special Purpose Services

This section describes services that are installed on systems that specifically need to run these services. If any of these services are not required, it is recommended that they be deleted from the system to reduce the potential attack surface. If a package is required as a dependency, and the service is not required, the service should be stopped and masked.

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

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

DRAFT

## *2.2.1 Ensure X Window System is not installed (Automated)*

### **Profile Applicability:**

- Level 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:**

Many Linux systems run applications which require a Java runtime. Some Linux Java packages have a dependency on specific X Windows xorg-x11-fonts. One workaround to avoid this dependency is to use the "headless" Java packages for your specific Java runtime, if provided by your distribution.

### **Audit:**

Verify X Windows System is not installed:

```
dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n' xserver-xorg* | grep -Pi '\h+installed\b'
```

Nothing should be returned

### **Remediation:**

Remove the X Windows System packages:

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

### **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>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, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

## 2.2.2 Ensure Avahi Server is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine.

### Rationale:

Automatic discovery of network services is not normally required for system functionality. It is recommended to remove this package to reduce the potential attack surface.

### Audit:

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
avahi-daemon  
  
avahi-daemon      unknown ok not-installed          not-installed
```

### Remediation:

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

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

### 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

## 2.2.3 Ensure CUPS is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

### Description:

The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability.

### Rationale:

If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be removed to reduce the potential attack surface.

### Impact:

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

### Audit:

Run the following command to verify cups is not Installed:

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n' cups
cups      unknown  ok  not-installed          not-installed
```

### Remediation:

Run one of the following commands to remove cups :

```
# apt purge cups
```

### References:

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

## 2.2.4 Ensure DHCP Server is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses.

### Rationale:

Unless a system is specifically set up to act as a DHCP server, it is recommended that this package be removed to reduce the potential attack surface.

### Audit:

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n' isc-dhcp-server
isc-dhcp-server      unknown  ok  not-installed      not-installed
```

### Remediation:

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

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

### References:

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

## 2.2.5 Ensure LDAP server is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

### Rationale:

If the system will not need to act as an LDAP server, it is recommended that the software be removed to reduce the potential attack surface.

### Audit:

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db>Status-Status}\n'  
slapd  
  
slapd    unknown  ok  not-installed          not-installed
```

### Remediation:

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

```
# apt purge slapd
```

### References:

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

## 2.2.6 Ensure NFS is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

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

### Rationale:

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

### Audit:

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n' nfs-kernel-server
nfs-kernel-server      unknown ok not-installed      not-installed
```

### Remediation:

Run the following command to remove `nfs`:

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

### 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 <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>		●	●

## 2.2.7 Ensure DNS Server is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network.

### Rationale:

Unless a system is specifically designated to act as a DNS server, it is recommended that the package be deleted to reduce the potential attack surface.

### Audit:

Run the following command to verify `DNS server` is not installed:

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
bind9  
bind9      unknown  ok    not-installed          not-installed
```

### Remediation:

Run the following commands to disable `DNS server`:

```
# apt purge bind9
```

### 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

## 2.2.8 Ensure FTP Server is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files.

### Rationale:

FTP does not protect the confidentiality of data or authentication credentials. It is recommended SFTP be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be deleted to reduce the potential attack surface.

### Audit:

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
vsftpd      unknown ok not-installed          not-installed
```

### Remediation:

Run the following command to remove `vsftpd`:

```
# apt purge vsftpd
```

### 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	<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

## 2.2.9 Ensure HTTP server is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

HTTP or web servers provide the ability to host web site content.

### Rationale:

Unless there is a need to run the system as a web server, it is recommended that the package be deleted to reduce the potential attack surface.

### Audit:

Run the following command to verify `apache2` is not installed:

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
apache2  
apache2      unknown ok not-installed          not-installed
```

### Remediation:

Run the following command to remove `apache2`:

```
# apt purge apache2
```

### 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	<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

## *2.2.10 Ensure IMAP and POP3 server are not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

dovecot-imapd and dovecot-pop3d are an open source IMAP and POP3 server for Linux based systems.

### **Rationale:**

Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the package be removed to reduce the potential attack surface.

### **Audit:**

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
dovecot-imapd dovecot-pop3d  
  
dovecot-imapd      unknown ok not-installed      not-installed  
dovecot-pop3d      unknown ok not-installed      not-installed
```

### **Remediation:**

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

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

### **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	<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

## 2.2.11 Ensure Samba is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Server Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems.

### Rationale:

If there is no need to mount directories and file systems to Windows systems, then this service should be deleted to reduce the potential attack surface.

### Audit:

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
samba  
  
samba      unknown  ok  not-installed          not-installed
```

### Remediation:

Run the following command to remove `samba`:

```
# apt purge samba
```

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

## 2.2.12 Ensure HTTP Proxy Server is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Squid is a standard proxy server used in many distributions and environments.

### Rationale:

If there is no need for a proxy server, it is recommended that the squid proxy be deleted to reduce the potential attack surface.

### Audit:

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

```
# dpkg-query -W -f='${binary:Package}\t${status}\t${db:Status-Status}\n'  
squid  
  
squid    unknown  ok  not-installed          not-installed
```

### Remediation:

Run the following command to remove `squid`:

```
# apt purge squid
```

### References:

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

## 2.2.13 Ensure SNMP Server is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

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

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

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

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

### Rationale:

The SNMP server can communicate using `SNMPv1`, which transmits data in the clear and does not require authentication to execute commands. `SNMPv3` replaces the simple/clear text password sharing used in `SNMPv2` with more securely encoded parameters. If the the SNMP service is not required, the `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.

## Audit:

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
snmpd  
  
snmpd    unknown  ok  not-installed          not-installed
```

## Remediation:

Run the following command to remove `snmpd`:

```
# apt purge snmpd
```

## 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

## 2.2.14 Ensure NIS Server is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files.

### Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed and other, more secure services be used

### Audit:

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db>Status-Status}\n' nis
nis      unknown ok not-installed          not-installed
```

### Remediation:

Run the following command to remove `nis`:

```
# apt purge nis
```

### 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, T1543, T1543.002	TA0008	M1042

## 2.2.15 Ensure `dnsmasq` is not installed (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.

### Audit:

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
dnsmasq      unknown ok not-installed          not-installed
```

### Remediation:

Run the following command to remove `dnsmasq`:

```
# apt purge dnsmasq
```

### 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

## *2.2.16 Ensure mail transfer agent is configured for local-only mode (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.

### **Rationale:**

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

### **Note:**

- This recommendation is designed around the 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.

### **Audit:**

Run the following command to verify that the MTA is not listening on any non-loopback address (127.0.0.1 or ::1).

```
# ss -lntu | grep -P ':25\b' | grep -Pv '\h+(127\.0\.0\.1|::1)\?':25\b'
```

Nothing should be returned

## 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
```

## 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

## *2.2.17 Ensure telnetd is not installed (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must not have the telnet package installed.

### **Rationale:**

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

### **Audit:**

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

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

If the package is installed, this is a finding.

### **Remediation:**

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

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

### **References:**

1. NIST SP 800-53 Revision 4 :: IA-5 (1) (c)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238326

Rule ID: SV-238326r654153\_rule

STIG ID: UBTU-20-010405

Severity: CAT I

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.		●	●

## *2.2.18 Ensure rsync service is either not installed or is masked (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

The `rsync` service presents a security risk as the `rsync` protocol is unencrypted. The `rsync` package should be removed or if required for dependencies, the `rsync` service should be stopped and masked to reduce the attack area of the system.

### **Audit:**

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

```
dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n' rsync
rsync      unknown ok not-installed          not-installed
```

-- OR --

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

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

## Remediation:

Run the following command to remove `rsync`:

```
# apt purge rsync
```

-- OR --

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

```
# systemctl stop rsync  
# systemctl mask rsync
```

## References:

1. NIST SP 800-53 Rev. 5: CM-6, 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
T1105, T1105.000, T1203, T1203.000, T1210, T1210.000, T1543, T1543.002, T1570, T1570.000	TA0008	M1042

## *2.2.19 Ensure rsh-server is not installed (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must not have the rsh-server package installed.

### **Rationale:**

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software, not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

### **Audit:**

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

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

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

### **Remediation:**

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

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

### **References:**

1. NIST SP 800-53 Revision 5 :: CM-7 a

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238327

Rule ID: SV-238327r654156\_rule

STIG ID: UBTU-20-010406

Severity: CAT I

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.		●	●

## 2.3 Service Clients

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

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

DRAFT

### *2.3.1 Ensure NIS Client is not installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client was used to bind a machine to an NIS server and receive the distributed configuration files.

#### **Rationale:**

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

#### **Impact:**

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

#### **Audit:**

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n' nis
nis      unknown ok not-installed          not-installed
```

#### **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

## 2.3.2 Ensure rsh client is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

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

### Rationale:

These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the `rsh-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 -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n' rsh-client
rsh-client      unknown ok not-installed      not-installed
```

### 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

### *2.3.3 Ensure talk client is not installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Impact:**

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

#### **Audit:**

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

```
# dpkg-query -W -f='${binary:Package}\t${status}\t${db:Status-Status}\n' talk
talk      unknown ok not-installed          not-installed
```

#### **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

## *2.3.4 Ensure telnet client is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `telnet` package contains the `telnet` client, which allows users to start connections to other systems via the telnet protocol.

### **Rationale:**

The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The `ssh` package provides an encrypted session and stronger security and is included in most Linux distributions.

### **Impact:**

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

### **Audit:**

Verify `telnet` is not installed. Use the following command to provide the needed information:

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
telnet  
  
telnet      unknown  ok  not-installed          not-installed
```

### **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

### *2.3.5 Ensure LDAP client is not installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

#### **Rationale:**

If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.

#### **Impact:**

Removing the LDAP client will prevent or inhibit using LDAP for authentication in your environment.

#### **Audit:**

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
ldap-utils
```

ldap-utils	unknown	ok	not-installed	not-installed
------------	---------	----	---------------	---------------

#### **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

## 2.3.6 Ensure RPC is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

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

### Rationale:

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

### Audit:

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

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db>Status-Status}\n'  
rpcbind  
rpcbind      unknown ok not-installed          not-installed
```

### Remediation:

Run the following command to remove `rpcbind`:

```
# apt purge rpcbind
```

### 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, T1543, T1543.002	TA0008	M1042

## *2.4 Ensure nonessential services are removed or masked (Manual)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

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

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

### **Rationale:**

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

## Audit:

Run the following command:

```
# ss -plntu
```

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

## Remediation:

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

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

*OR If required packages have a dependency:*

Run the following commands to stop and mask the service:

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

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

DRAFT

## **3 Network**

This section provides guidance on for securing the network configuration of the system.

DRAFT

### 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.

DRAFT

### *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 - IPv6 is enabled\n" || echo -e "\n - IPv6 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

DRAFT

### *3.1.2 Ensure wireless interfaces are disabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- STIG

#### **Description:**

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

#### **Rationale:**

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

#### **Impact:**

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

## Audit:

Run the following script to verify no wireless interfaces are active on the system:

```
#!/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:\n$l_output2\n"
        [ -n "$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 "$1_mname" | grep -P -- '^h*install
\bin\/(true|false)'; then
            echo -e " - setting module: \"$1_mname\" to be un-loadable"
            echo -e "install $1_mname /bin/false" >>
/etc/modprobe.d/"$1_mname".conf
        fi
        if lsmod | grep "$1_mname" > /dev/null 2>&1; then
            echo -e " - unloading module \"$1_mname\""
            modprobe -r "$1_mname"
        fi
        if ! grep -Pq -- '^h*blacklist\h+$1_mname\b' /etc/modprobe.d/*; then
            echo -e " - deny listing \"$1_mname\""
            echo -e "blacklist $1_mname" >> /etc/modprobe.d/"$1_mname".conf
        fi
    }
    if [ -n "$(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

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-252704  
Rule ID: SV-252704r916433\_rule  
STIG ID: UBTU-20-010455  
Severity: CAT II

## 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 -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
bluez  
  
bluez      unknown  ok  not-installed          not-installed
```

-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 <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>		●	●

## 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.

DRAFT

### *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	<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
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

### *3.2.2 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 \\\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

### *3.2.3 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 \\\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	<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
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

### **3.2.4 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 \\\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	<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
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 logically 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 "$l_output" ] && echo -e "\n- Correctly set:\n$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.ip_forward = 0`

### *Example:*

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

Run the following command to set the active kernel parameters:

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

-IF- IPv6 is enabled on the system:

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

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

### *Example:*

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

Run the following command to set the active kernel parameters:

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

**Note:** If these settings appear in a conically 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	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></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

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

Run the following command to set the active kernel parameters:

```
# {  
    sysctl -w net.ipv4.conf.all.send_redirects=0  
    sysctl -w net.ipv4.conf.default.send_redirects=0  
    sysctl -w net.ipv4.route.flush=1  
}
```

**Note:** If these settings appear in a conically 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 conically 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 "  
net.ipv4.icmp_ignore_bogus_error_responses = 1  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

**Note:** If these settings appear in a conically 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 conically 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" = "$l_kpname" ]; then
            l_output="$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_kpname\""
        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" = "$l_kpvvalue" ]; then
                    l_output="$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_kpvvalue\"\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\"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS="=" read -r l_kpname l_kpvvalue; do # Assess and check parameters
        l_kpname="${l_kpname// /}"; l_kpvvalue="${l_kpvvalue// /}"
        if ! grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && grep -q '^net.ipv6.' <<< "$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_echo_ignore_broadcasts = 1`

### *Example:*

```
# printf "\nnet.ipv4.icmp_echo_ignore_broadcasts = 1\n" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

**Note:** If these settings appear in a conically 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 logically 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 "  
net.ipv4.conf.all.accept_redirects = 0  
net.ipv4.conf.default.accept_redirects = 0  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {  
    sysctl -w net.ipv4.conf.all.accept_redirects=0  
    sysctl -w net.ipv4.conf.default.accept_redirects=0  
    sysctl -w net.ipv4.route.flush=1  
}
```

**-IF- IPv6 is enabled on the system:**

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

- net.ipv6.conf.all.accept\_redirects = 0
- net.ipv6.conf.default.accept\_redirects = 0

### **Example:**

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

Run the following command to set the active kernel parameters:

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

**Note:** If these settings appear in a conically 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 conically 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: \"$l_kpname\" May be set in a file that's ignored by load procedure **\n"
        fi
    }
    while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
        l_kpname="${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.secure_redirects = 0`
- `net.ipv4.conf.default.secure_redirects = 0`

## **Example:**

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

Run the following commands to set the active kernel parameters:

```
# {  
    sysctl -w net.ipv4.conf.all.secure_redirects=0  
    sysctl -w net.ipv4.conf.default.secure_redirects=0  
    sysctl -w net.ipv4.route.flush=1  
}
```

**Note:** If these settings appear in a conically 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></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
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 conically 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 "  
net.ipv4.conf.all.rp_filter = 1  
net.ipv4.conf.default.rp_filter = 1  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following commands to set the active kernel parameters:

```
# {  
    sysctl -w net.ipv4.conf.all.rp_filter=1  
    sysctl -w net.ipv4.conf.default.rp_filter=1  
    sysctl -w net.ipv4.route.flush=1  
}
```

**Note:** If these settings appear in a conically 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 tcp syn Cookies is enabled (Automated)*

#### **Profile Applicability:**

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

#### **Description:**

When `tcp_syncookies` is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

#### **Rationale:**

Attackers use SYN flood attacks to perform a denial of service attack on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

## Audit:

Run the following commands and verify output matches:

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

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.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 logically 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.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 '\n%s' "net.ipv4.tcp_syncookies = 1" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

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

## **References:**

1. NIST SP 800-53 Revision 5 :: SC-5 (2)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238333  
Rule ID: SV-238333r654174\_rule  
STIG ID: UBTU-20-010412  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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	TA0006, TA0009	M1030, M1042

DRAFT

### *3.3.9 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 logically 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* 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]+|[^\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
    done
}

```

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

Run the following command to set the active kernel parameters:

```
# {  
    sysctl -w net.ipv4.conf.all.accept_source_route=0  
    sysctl -w net.ipv4.conf.default.accept_source_route=0  
    sysctl -w net.ipv4.route.flush=1  
}
```

**-IF- IPv6 is enabled on the system:**

**Set the following parameters in /etc/sysctl.conf or a 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 "  
net.ipv6.conf.all.accept_source_route = 0  
net.ipv6.conf.default.accept_source_route = 0  
" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

**Note:** If these settings appear in a conically 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	

### 3.3.10 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 conically 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 "$l_output" ] && echo -e "\n- Correctly set:\n$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.log_martians = 1`
- `net.ipv4.conf.default.log_martians = 1`

## **Example:**

```
# printf "  
net.ipv4.conf.all.log_martians = 1  
net.ipv4.conf.default.log_martians = 1  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {  
    sysctl -w net.ipv4.conf.all.log_martians=1  
    sysctl -w net.ipv4.conf.default.log_martians=1  
    sysctl -w net.ipv4.route.flush=1  
}
```

**Note:** If these settings appear in a conically 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	

### *3.3.11 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 logically 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 (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
            while IFS= "=" read -r l_fkpname l_fkpvalue; do
                l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
                if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                    l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$(printf '%s' "${A_out[@]}")\"\n"
                else
                    l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_fkpvalue\" in \"$(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:

**-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 "
net.ipv6.conf.all.accept_ra = 0
net.ipv6.conf.default.accept_ra = 0
" >> /etc/sysctl.d/60-netipv6_sysctl.conf

```

Run the following command to set the active kernel parameters:

```

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

```

**Note:** If these settings appear in a conically 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	<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, TA0040	M1030, M1042

### 3.4 Configure 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

### 3.4.1 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.

### *3.4.1.1 Ensure ufw is installed (Automated)*

#### **Profile Applicability:**

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

#### **Description:**

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

#### **Rationale:**

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

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

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

#### **Audit:**

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

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

#### **Remediation:**

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

```
apt install ufw
```

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238354

Rule ID: SV-238354r654237\_rule

STIG ID: UBTU-20-010433

Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●
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.	●	●	●

### **3.4.1.2 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  
package 'iptables-persistent' is not installed and no information is available
```

#### **Remediation:**

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

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

#### **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	

### *3.4.1.3 Ensure ufw service is enabled (Automated)*

#### **Profile Applicability:**

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

#### **Description:**

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

#### **Notes:**

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

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

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

#### **Rationale:**

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

#### **Impact:**

Changing firewall settings while connected over network can result in being locked out of the system.

## Audit:

Run the following command to verify that ufw is enabled:

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

Run the following command to verify that ufw is running:

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

## Remediation:

Run the following command to enable ufw:

```
# ufw enable
```

## References:

1. <http://manpages.ubuntu.com/manpages/precise/en/man8/ufw.8.html>
2. NIST SP 800-53 Revision 5 :: AC-17 (1)

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238355  
Rule ID: SV-238355r654240\_rule  
STIG ID: UBTU-20-010434  
Severity: CAT II

Vul ID: V-238374  
Rule ID: SV-238374r654297\_rule  
STIG ID: UBTU-20-010454  
Severity: CAT II

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●
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.	●	●	●

### **3.4.1.4 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

### *3.4.1.5 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

### *3.4.1.6 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: ${printf '%s\n' \"${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

### 3.4.1.7 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 git
ufw allow in http
ufw allow out http <- required for apt to connect to repository
ufw allow in https
ufw allow out https
ufw allow out 53
ufw logging on
```

#### Audit:

Run the following command and verify that the default policy for **incoming** , **outgoing** , and **routed** directions is **deny** , **reject** , or **disabled**:

```
# ufw status verbose | grep Default:
```

*Example output:*

```
Default: deny (incoming), deny (outgoing), disabled (routed)
```

## Remediation:

Run the following commands to implement a default *deny* policy:

```
# ufw default deny incoming  
# ufw default deny outgoing  
# ufw default deny routed
```

## 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

### **3.4.1.8 Ensure UFW rate-limits impacted network interfaces (Manual)**

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must configure the uncomplicated firewall to rate-limit impacted network interfaces.

#### **Rationale:**

Denial of service (DoS) is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

#### **Audit:**

Verify an application firewall is configured to rate limit any connection to the system. Check all the services listening to the ports with the following command:

```
# ss -l46ut  
  
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process  
tcp LISTEN 0 128 [::]:ssh [::]:*
```

For each entry, verify that the Uncomplicated Firewall is configured to rate limit the service ports with the following command:

```
# ufw status  
  
Status: active  
  
To Action From  
-- -----  
22/tcp LIMIT Anywhere  
22/tcp (v6) LIMIT Anywhere (v6)
```

If any port with a state of "LISTEN" is not marked with the "LIMIT" action, this is a finding.

## **Remediation:**

Configure the application firewall to protect against or limit the effects of DoS attacks by ensuring the Ubuntu operating system is implementing rate-limiting measures on impacted network interfaces.

Check all the services listening to the ports with the following command:

```
# ss -l46ut  
  
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process  
tcp LISTEN 0 128 [::]:ssh [::]:*
```

For each service with a port listening to connections, run the following command, replacing "[service]" with the service that needs to be rate limited.

```
# ufw limit [service]
```

Rate-limiting can also be done on an interface. An example of adding a rate-limit on the eth0 interface follows:

```
# ufw limit in on eth0
```

## **References:**

1. NIST SP 800-53 Revision 5 :: SC-5 a
2. NIST SP 800-53 Revision 4 :: SC-5

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238367  
Rule ID: SV-238367r654276\_rule  
STIG ID: UBTU-20-010446  
Severity: CAT II

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>	●	●	●
v7	<p><b>12.4 Deny Communication over Unauthorized Ports</b>            Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.</p>	●	●	●

### 3.4.2 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"
```

### 3.4.2.1 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 | grep 'Status: install ok installed'  
Status: install ok installed
```

#### Remediation:

Run the following command to install nftables:

```
# apt install 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

### **3.4.2.2 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 -W -f='${binary:Package}\t${Status}\t${db>Status-Status}\n' ufw  
dpkg-query: no packages found matching ufw
```

**-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	<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	

### 3.4.2.3 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	

### **3.4.2.4 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 build, nftables will not filter network traffic.

#### **Impact:**

Adding rules to a running nftables can cause loss of connectivity to the system

#### **Audit:**

Run the following command to verify that a nftables table exists:

```
# nft list tables
```

Return should include a list of nftables:

*Example:*

```
table inet filter
```

#### **Remediation:**

Run the following command to create a table in nftables

```
# nft create table inet <table name>
```

*Example:*

```
# nft create table inet filter
```

#### **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

### 3.4.2.5 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 \; }
```

## 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	

### 3.4.2.6 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 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	

### *3.4.2.7 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:**

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

DRAFT

### 3.4.2.8 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:**

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

DRAFT

### **3.4.2.9 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

### *3.4.2.10 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

DRAFT

### 3.4.3 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

### **3.4.3.1 Configure iptables software**

This section provides guidance for installing, enabling, removing, and disabling software packages necessary for using IPTables as the method for configuring and maintaining a Host Based Firewall on the system.

*Note: Using more than one method to configure and maintain a Host Based Firewall can cause unexpected results. If FirewallD or NFTables are being used for configuration and maintenance, this section should be skipped and the guidance in their respective section followed.*

DRAFT

### **3.4.3.1.1 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* and *iptables-persistent* are installed:

```
# apt list iptables iptables-persistent | grep installed  
iptables-persistent/<version> [installed,automatic]  
iptables/<version> [installed,automatic]
```

#### **Remediation:**

Run the following command to install *iptables* and *iptables-persistent*

```
# apt install iptables iptables-persistent
```

#### **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

### **3.4.3.1.2 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 -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
nftables  
nftables      unknown  ok  not-installed          not-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	

### **3.4.3.1.3 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 -W -f='${binary:Package}\t${Status}\t${db>Status-Status}\n' ufw  
ufw      unknown ok not-installed          not-installed
```

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: 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	

### 3.4.3.2 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
```

### 3.4.3.2.1 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 -n
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

### **3.4.3.2.2 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 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

### **3.4.3.2.3 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

### *3.4.3.2.4 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

### 3.4.3.3 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
```

### *3.4.3.3.1 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 -n
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	<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

### *3.4.3.3.2 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

### *3.4.3.3 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

### *3.4.3.3.4 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 DROP       all    *       *       ::/1
  0      0 ACCEPT     tcp    *       *       ::/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 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:**

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	<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 Access, Authentication and Authorization

DRAFT

## **4.1 Configure job schedulers**

A job scheduler is used to execute jobs, commands, or shell scripts, at fixed times, dates, or intervals

DRAFT

#### 4.1.1 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

#### *4.1.1.1 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:**

Run the following command to verify `cron` is enabled:

```
# systemctl is-enabled cron  
enabled
```

Run the following command to verify that `cron` is active:

```
# systemctl is-active cron  
active
```

##### **Remediation:**

Run the following commands to unmask, enable, and start `cron`:

```
# systemctl unmask cron  
# systemctl --now enable cron
```

##### **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
T1562, T1562.001	TA0005	M1018

#### *4.1.1.2 Ensure permissions on /etc/crontab are configured (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The `/etc/crontab` file is used by `cron` to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file.

##### **Rationale:**

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

##### **Audit:**

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group or other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/crontab
Access: (600/-rw-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

##### **Remediation:**

Run the following commands to set ownership and permissions on `/etc/crontab`:

```
# chown root:root /etc/crontab
# chmod og-rwx /etc/crontab
```

##### **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

#### *4.1.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

This directory contains system `cron` jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

##### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

##### **Audit:**

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.hourly/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

##### **Remediation:**

Run the following commands to set ownership and permissions on the `/etc/cron.hourly` directory:

```
# chown root:root /etc/cron.hourly/  
# chmod og-rwx /etc/cron.hourly/
```

##### **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

#### *4.1.1.4 Ensure permissions on /etc/cron.daily are configured (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The `/etc/cron.daily` directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

##### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

##### **Audit:**

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.daily/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

##### **Remediation:**

Run the following commands to set ownership and permissions on the `/etc/cron.daily` directory:

```
# chown root:root /etc/cron.daily/  
# chmod og-rwx /etc/cron.daily/
```

##### **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

#### *4.1.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The `/etc/cron.weekly` directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

##### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

##### **Audit:**

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.weekly/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

##### **Remediation:**

Run the following commands to set ownership and permissions on the `/etc/cron.weekly` directory:

```
# chown root:root /etc/cron.weekly/  
# chmod og-rwx /etc/cron.weekly/
```

##### **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

#### *4.1.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The `/etc/cron.monthly` directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

##### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

##### **Audit:**

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.monthly/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

##### **Remediation:**

Run the following commands to set ownership and permissions on the `/etc/cron.monthly` directory:

```
# chown root:root /etc/cron.monthly/  
# chmod og-rwx /etc/cron.monthly/
```

##### **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

#### *4.1.1.7 Ensure permissions on /etc/cron.d are configured (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The `/etc/cron.d` directory contains system cron jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from `/etc/crontab`, but require more granular control as to when they run. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

##### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

##### **Audit:**

Run the following command and verify Uid and Gid are both 0/root and Access does not grant permissions to group or other:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.d/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

##### **Remediation:**

Run the following commands to set ownership and permissions on the `/etc/cron.d` directory:

```
# chown root:root /etc/cron.d/  
# chmod og-rwx /etc/cron.d/
```

##### **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

#### *4.1.1.8 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 setup 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 `crontab`

```
# stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/cron.allow
Access: (640/-rw-r-----) Owner: (root) Group: (crontab)
```

Run the following command to verify `cron.deny` doesn't exist, -OR- is:

- Mode 0640 or more restrictive
- Owned by the user `root`
- Group owned by the group `crontab`

```
# [ -e "/etc/cron.deny" ] && stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/cron.deny
Access: (640/-rw-r-----) Owner: (root) Group: (crontab)
-OR-
Nothing is returned
```

## **Remediation:**

**-IF-** cron is installed on the system:

Run the following commands to:

- Create `/etc/cron.allow` if it doesn't exist
- Change owner or user `root`
- Change group owner to group `crontab`
- Change mode to `640` or more restrictive

```
# [ ! -e "/etc/cron.allow" ] && touch /etc/cron.allow
# chown root:crontab /etc/cron.allow
# chmod u-x,g-wx,o-rwx /etc/cron.allow
```

Run the following commands to:

**-IF-** `/etc/cron.deny` exists:

- Change owner or user `root`
- Change group owner to group `crontab`
- Change mode to `640` or more restrictive

```
# [ -e "/etc/cron.deny" ] && chown root:crontab /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:**

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002	M1018

DRAFT

#### 4.1.2 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

DRAFT

#### *4.1.2.1 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)
```

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-  
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/cron.deny
    [ -e "/etc/at.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	<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	M1018

## 4.2 Configure SSH Server

SSH is a secure, encrypted replacement for common login services such as `telnet`, `ftp`, `rlogin`, `rsh`, and `rcp`. It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

### Note:

- The recommendations in this section only apply if the SSH daemon is installed on the system, if remote access is **not** required the SSH daemon can be removed and this section skipped.
- The following openSSH daemon configuration options, `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.
- Once all configuration changes have been made to `/etc/ssh/sshd_config` or any included configuration files, the `sshd` configuration must be reloaded
- `Include`:
  - Include the specified configuration file(s).
  - Multiple pathnames may be specified and each pathname may contain `glob(7)` wildcards.
  - 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`, `RDomain`, and `Address` (with

- RDomain representing the rdomain(4) on which the connection was received).
- 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: AcceptEnv, AllowAgentForwarding, AllowGroups, AllowStreamLocalForwarding, AllowTcpForwarding, AllowUsers, AuthenticationMethods, AuthorizedKeysCommand, AuthorizedKeysCommandUser, AuthorizedKeysFile, AuthorizedPrincipalsCommand, AuthorizedPrincipalsCommandUser, AuthorizedPrincipalsFile, Banner, ChrootDirectory, ClientAliveCountMax, ClientAliveInterval, DenyGroups, DenyUsers, ForceCommand, GatewayPorts, GSSAPIAuthentication, HostbasedAcceptedKeyTypes, HostbasedAuthentication, HostbasedUsesNameFromPacketOnly, Include, IPQoS, KbdInteractiveAuthentication, KerberosAuthentication, LogLevel, MaxAuthTries, MaxSessions, PasswordAuthentication, PermitEmptyPasswords, PermitListen, PermitOpen, PermitRootLogin, PermitTTY, PermitTunnel, PermitUserRC, PubkeyAcceptedKeyTypes, PubkeyAuthentication, RekeyLimit, RevokedKeys, RDomain, SetEnv, StreamLocalBindMask, StreamLocalBindUnlink, TrustedUserCAKeys, X11DisplayOffset, X11Forwarding and X11UseLocalhost.

Command to re-load the SSH daemon configuration:

```
# systemctl reload sshd
```

Command to remove the SSH daemon:

```
# apt purge openssh-server
```

#### *4.2.1 Ensure SSH is installed and active (Automated)*

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

- STIG

##### **Description:**

The operating system must use SSH to protect the confidentiality and integrity of transmitted information.

##### **Rationale:**

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

## Audit:

Verify the SSH package is installed with the following command:

```
# dpkg -l | grep openssh  
  
ii  openssh-client 1:7.6p1-4ubuntu0.1 amd64  secure shell (SSH) client, for  
secure access to remote machines  
ii  openssh-server 1:7.6p1-4ubuntu0.1 amd64  secure shell (SSH) server, for  
secure access from remote machines  
ii  openssh-sftp-server 1:7.6p1-4ubuntu0.1 amd64  secure shell (SSH) sftp  
server module, for SFTP access from remote machines
```

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

Verify the "sshd.service" is loaded and active with the following command:

```
# systemctl status sshd.service | egrep -i "(active|loaded)"  
  
Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset:  
enabled)  
Active: active (running) since Thu 2019-01-24 22:52:58 UTC; 1 weeks 3 days  
ago
```

If "sshd.service" is not active or loaded, this is a finding.

## Remediation:

Install the "ssh" meta-package on the system with the following command:

```
# apt install ssh
```

Enable the "ssh" service to start automatically on reboot with the following command:

```
# systemctl enable sshd.service
```

ensure the "ssh" service is running

```
# systemctl start sshd.service
```

## References:

1. NIST SP 800-53 Revision 4 :: SC-8

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238215  
Rule ID: SV-238215r916422\_rule  
STIG ID: UBTU-20-010042  
Severity: CAT I

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

## 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.		●	●

DRAFT

#### *4.2.2 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/sshd_config.d` 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=""
    unset a_sshdfiles && a_sshdfiles=()
    [ -e "/etc/ssh/sshd_config" ] && a_sshdfiles+=("$(stat -Lc '%n^%#a^%U^%G' '/etc/ssh/sshd_config')")
    while IFS= read -r -d $'\0' l_file; do
        [ -e "$l_file" ] && a_sshdfiles+=("$(stat -Lc '%n^%#a^%U^%G' \"$l_file\")")
    done < <(find /etc/ssh/sshd_config.d -type f \(\ -perm /077 -o ! -user root -o ! -group root \) -print0)
    if (( ${#a_sshdfiles[@]} != 0 )); then
        perm_mask='0177'
        maxperm=$( printf '%o' $(( 0777 & ~$perm_mask)) )
        while IFS="^" read -r l_file 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\":$l_out2"
            fi
        done <<< "$(printf '%s\n' "${a_sshdfiles[@]}")"
        fi
        unset a_sshdfiles
        # If l_output2 is empty, we pass
        if [ -z "$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
    }
}
```

## 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)
}
```

## 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

#### *4.2.3 Ensure permissions on SSH private host key files are configured (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

An SSH private key is one of two files used in SSH public key authentication. In this authentication method, the possession of the private key is proof of identity. Only a private key that corresponds to a public key will be able to authenticate successfully. The private keys need to be stored and handled carefully, and no copies of the private key should be distributed.

##### **Rationale:**

If an unauthorized user obtains the private SSH host key file, the host could be impersonated

## Audit:

Run the following script to verify SSH private host key files are mode 0600 or more restrictive, owned by the root user, and owned by the group root or group designated to own openSSH private keys:

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

{
    l_output="" l_output2=""
    l_skgn="ssh_keys" # Group designated to own openSSH keys
    l_skgid=$(awk -F: '$1 == "'$l_skgn'" {print $3}' /etc/group) # Get gid of group
    [ -n "$l_skgid" ] && l_agroup="(root|$l_skgn)" || l_agroup="root"
    unset a_skarr && a_skarr=() # Clear and initialize array
    while IFS= read -r -d $'\0' l_file; do # Loop to populate array
        if grep -Pq ':hOpenSSH\h+private\h+key\b' <<< "${file "$l_file")"; then
            a_skarr+=("$(stat -Lc '%n^%#a^%U^%G^%g' "$l_file")")
        fi
    done <<(find -L /etc/ssh -xdev -type f -print0)
    while IFS="^" read -r l_file l_mode l_owner l_group l_gid; do
        echo "File: \"\$l_file\" Mode: \"\$l_mode\" Owner: \"\$l_owner\" Group: \"\$l_group\" GID: \"\$l_gid\""
        l_out2=""
        [ "\$l_gid" = "\$l_skgid" ] && l_pmask="0137" || l_pmask="0177"
        l_maxperm=$(( printf '%o' $(( 0777 & ~$l_pmask )) ))
        if [ $(( \$l_mode & $l_pmask )) -gt 0 ]; then
            l_out2="$l_out2\n - Mode: \"\$l_mode\" should be mode: \"\$l_maxperm\" or more restrictive"
        fi
        if [ "\$l_owner" != "root" ]; then
            l_out2="$l_out2\n - Owned by: \"\$l_owner\" should be owned by \"root\""
        fi
        if [[ ! "\$l_group" =~ \$l_agroup ]]; then
            l_out2="$l_out2\n - Owned by group \"\$l_group\" should be group owned by: \"\$l_agroup//\" or \"\$l_agroup"
        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_mode), owner (\$l_owner), and group owner (\$l_group) configured"
        fi
    done <<< "$(printf '%s\n' "${a_skarr[@]}")"
    unset a_skarr
    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
}
```

## 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_skgn="ssh_keys" # Group designated to own openSSH keys
    l_skgid=$(awk -F: '($1 == "'$l_skgn'") {print $3}' /etc/group) # Get gid of group
    if [ -n "$l_skgid" ]; then
        l_agroup="(root|$l_skgn)" && l_sgroup="$l_skgn" && l_mfix="u-x,g-wx,o-rwx"
    else
        l_agroup="root" && l_sgroup="root" && l_mfix="u-x,go-rwx"
    fi
    unset a_skarr && a_skarr=() # Clear and initialize array
    while IFS= read -r -d $'\0' l_file; do # Loop to populate array
        if grep -Pq ':\h+OpenSSH\h+private\h+key\b' <<< "$(file "$l_file")"; then
            a_skarr+=("$(stat -Lc '%n^%#a^%U^%G^%g' "$l_file")")
        fi
    done < <(find -L /etc/ssh -xdev -type f -print0)
    while IFS="^" read -r l_file l_mode l_owner l_group l_gid; do
        l_out2=""
        [ "$l_gid" = "$l_skgid" ] && l_pmask="0137" || l_pmask="0177"
        l_maxperm=$( printf '%o' $(( 0777 & ~$l_pmask )) )
        if [ $(( $l_mode & $l_pmask )) -gt 0 ]; then
            l_out2="$l_out2\n - Mode: \"$l_mode\" should be mode: \"$l_maxperm\" or more restrictive\n - Revoking excess permissions"
            chmod "$l_mfix" "$l_file"
        fi
        if [ "$l_owner" != "root" ]; then
            l_out2="$l_out2\n - Owned by: \"$l_owner\" should be owned by \"root\"\n - Changing ownership to \"root\""
            chown root "$l_file"
        fi
        if [[ ! "$l_group" =~ $l_agroup ]]; then
            l_out2="$l_out2\n - Owned by group \"$l_group\" should be group owned by: \"${l_agroup//|/} or ${l_agroup//|/}\n - Changing group ownership to \"$l_sgroup\""
            chgrp "$l_sgroup" "$l_file"
        fi
        [ -n "$l_out2" ] && l_output2="$l_output2\n - File: \"$l_file\"$l_out2"
    done <<< "$(printf '%s\n' "${a_skarr[@]}")"
    unset a_skarr
    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

#### *4.2.4 Ensure permissions on SSH public host key files are configured (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

An SSH public key is one of two files used in SSH public key authentication. In this authentication method, a public key is a key that can be used for verifying digital signatures generated using a corresponding private key. Only a public key that corresponds to a private key will be able to authenticate successfully.

##### **Rationale:**

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

##### **Audit:**

Run the following command and verify Access does not grant write or execute permissions to group or other for all returned files:

Run the following script to verify SSH public host key files are mode 0644 or more restrictive, owned be the root user, and owned be the root group:

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    l_pmask="0133"
    awk '{print}' <<< "$(
        find -L /etc/ssh -xdev -type f -exec stat -Lc "%n %#a %U %G" {} +)" |
        (while read -r l_file l_mode l_owner l_group; do
            if file "$l_file" | grep -Pq ':h+OpenSSH\h+(\H+\h+)?public\h+key\b';
            then
                l_maxperm=$( printf '%o' $(( 0777 & ~$l_pmask )) )
                if [ $(( $l_mode & $l_pmask )) -gt 0 ]; then
                    l_output2="$l_output2\n - Public key file: \"$l_file\" is mode
\"$l_mode\" should be mode: \"$l_maxperm\" or more restrictive"
                else
                    l_output="$l_output\n - Public key file: \"$l_file\" is mode
\"$l_mode\" should be mode: \"$l_maxperm\" or more restrictive"
                fi
                if [ "$l_owner" != "root" ]; then
                    l_output2="$l_output2\n - Public key file: \"$l_file\" is owned
by: \"$l_owner\" should be owned by \"root\""
                else
                    l_output="$l_output\n - Public key file: \"$l_file\" is owned by:
\"$l_owner\" should be owned by \"root\""
                fi
                if [ "$l_group" != "root" ]; then
                    l_output2="$l_output2\n - Public key file: \"$l_file\" is owned
by group \"$l_group\" should belong to group \"root\"\n"
                else
                    l_output="$l_output\n - Public key file: \"$l_file\" is owned by
group \"$l_group\" should belong to group \"root\"\n"
                fi
            fi
        done
        if [ -z "$l_output2" ]; then
            echo -e "\n- Audit Result:\n *** PASS ***\n$l_output"
        else
            echo -e "\n- Audit Result:\n *** FAIL ***\n$l_output2\n\n - Correctly
set:\n$l_output"
        fi
    )
}

```

## **Remediation:**

Run the following script to set mode, ownership, and group on the public SSH host key files:

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

{
    l_pmask="0133"
    l_maxperm=$( printf '%o' $(( 0777 & ~$l_pmask )) )
    awk '{print}' <<< "$(
        find -L /etc/ssh -xdev -type f -exec stat -Lc "%n %#a %U %G" {} +)" |
        (while read -r l_file l_mode l_owner l_group; do
            if file "$l_file" | grep -Pq ':h+OpenSSH\h+(\H+\h+)?public\h+key\b';
            then
                echo -e " - Checking private key file: \"$l_file\""
                if [ $(($l_mode & $l_pmask)) -gt 0 ]; then
                    echo -e " - File: \"$l_file\" is mode \"$l_mode\" changing to
mode: \"$l_maxperm\""
                    chmod u-x,go-wx "$l_file"
                fi
                if [ "$l_owner" != "root" ]; then
                    echo -e " - File: \"$l_file\" is owned by: \"$l_owner\" changing
owner to \"root\""
                    chown root "$l_file"
                fi
                if [ "$l_group" != "root" ]; then
                    echo -e " - File: \"$l_file\" is owned by group \"$l_group\""
                    chgrp "root" "$l_file"
                fi
            fi
        done
    )
}
```

## **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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

## MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0003, TA0006	M1022

#### *4.2.5 Ensure SSH access is limited (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

- AllowUsers:
  - The `AllowUsers` variable gives the system administrator the option of allowing specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of `user@host`.
- AllowGroups:
  - The `AllowGroups` variable gives the system administrator the option of allowing specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.
- DenyUsers:
  - The `DenyUsers` variable gives the system administrator the option of denying specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of `user@host`.
- DenyGroups:
  - The `DenyGroups` variable gives the system administrator the option of denying specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

##### **Rationale:**

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

## Audit:

Run the following commands and verify the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -Pi '^h*(allow|deny) (users|groups) \h+\H+(\h+.*?)$'  
  
# grep -Pis '^h*(allow|deny) (users|groups) \h+\H+(\h+.*?)$' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf
```

Verify that the output of both commands matches at least one of the following lines:

```
allowusers <userlist>  
allowgroups <grouplist>  
denyusers <userlist>  
denygroups <grouplist>
```

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or `Match` set statements are used in your environment, those locations should be checked for the correct configuration as well.

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set one or more of the parameter above any `Include` entries as follows:

```
AllowUsers <userlist>
```

OR

```
AllowGroups <grouplist>
```

OR

```
DenyUsers <userlist>
```

OR

```
DenyGroups <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 file in `Include` location. If the `Include` location is not the default, `/etc/ssh/sshd_config.d/*.conf`, the audit will need to be modified to account for the `Include` location used.

## Default Value:

None

## References:

1. [SSHD\\_CONFIG\(5\)](#)
2. [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

## 4.2.6 Ensure SSH LogLevel is appropriate (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

`INFO` level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

`VERBOSE` level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments.

### Rationale:

SSH provides several logging levels with varying amounts of verbosity. `DEBUG` is specifically **not** recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

### Audit:

Run the following command and verify that output matches `loglevel VERBOSE` or `loglevel INFO`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep loglevel  
loglevel VERBOSE or loglevel INFO
```

Run the following command and verify the output matches:

```
# grep -Pis '^h*loglevel\h+' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf | grep -Pvi '(VERBOSE|INFO)'  
Nothing should be returned
```

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or `Match` set statements are used in your environment, those locations should be checked for the correct configuration as well.

## **Remediation:**

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

`LogLevel VERBOSE`

*OR*

`LogLevel INFO`

**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:**

`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	

#### 4.2.7 Ensure SSH PAM is enabled (Automated)

##### Profile Applicability:

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

##### Description:

The `UsePAM` directive enables the Pluggable Authentication Module (PAM) interface. If set to `yes` this will enable PAM authentication using `ChallengeResponseAuthentication` and `PasswordAuthentication` directives in addition to PAM account and session module processing for all authentication types.

##### Rationale:

When `usePAM` is set to `yes`, PAM runs through account and session types properly. This is important if you want to restrict access to services based off of IP, time or other factors of the account. Additionally, you can make sure users inherit certain environment variables on login or disallow access to the server

##### Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i usepam
```

Verify the output matches:

```
usepam yes
```

Run the following command:

```
# grep -Pis '^h*UsePAM\h+?"no"?\\b' /etc/ssh/sshd_config /etc/ssh/ssh_config.d/*.conf
```

Nothing should be returned.

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` are used in your environment, those locations should be checked for the correct configuration as well.

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
UsePAM 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. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238211  
Rule ID: SV-238211r877395\_rule  
STIG ID: UBTU-20-010035  
Severity: CAT II

## 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, T1021.004	TA0001	M1035

## 4.2.8 Ensure SSH root login is disabled (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `PermitRootLogin` parameter specifies if the root user can log in using SSH. The default is `prohibit-password`.

### Rationale:

Disallowing `root` logins over SSH requires system admins to authenticate using their own individual account, then escalating to `root`. This limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident.

### Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permitrootlogin
```

Verify the output matches:

```
permitrootlogin no
```

Run the following command:

```
# grep -Pis '^h*PermitRootLogin\h+?(yes|prohibit-password|forced-commands-only)\b' /etc/ssh/sshd_config /etc/ssh/ssh_config.d/*.conf
```

Nothing should be returned.

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or `Match` set statements are used in your environment, those locations should be checked for the correct configuration as well.

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
PermitRootLogin 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:

`PermitRootLogin without-password`

## References:

1. SSHD\_CONFIG(5)

## 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
T1021	TA0008	M1042

## 4.2.9 Ensure SSH HostbasedAuthentication is disabled (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `HostbasedAuthentication` parameter specifies if authentication is allowed through trusted hosts via the user of `.rhosts`, or `/etc/hosts.equiv`, along with successful public key client host authentication.

### Rationale:

Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, disabling the ability to use `.rhosts` files in SSH provides an additional layer of protection.

### Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep hostbasedauthentication
```

Verify the output matches:

```
hostbasedauthentication no
```

Run the following command:

```
# grep -Pis '^h*HostbasedAuthentication\h+?"yes"?\\b' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf
```

Nothing should be returned.

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or `Match` set statements are used in your environment, those locations should be checked for the correct configuration as well.

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` 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)

**MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0001	M1042

## 4.2.10 Ensure SSH PermitEmptyPasswords is disabled (Automated)

### Profile Applicability:

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

### Description:

The `PermitEmptyPasswords` parameter specifies if the SSH server allows login to accounts with empty password strings.

### Rationale:

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system.

### Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permitemptypasswords
```

Verify the output matches:

```
permitemptypasswords no
```

Run the following command and verify the output:

```
# grep -Pis '^h*PermitEmptyPasswords\h+?yes\b' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf
```

Nothing should be returned.

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or `Match` set statements are used in your environment, those locations should be checked for the correct configuration as well.

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
PermitEmptyPasswords 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:**

PermitEmptyPasswords no

**References:**

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 :: CM-6

**Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238218

Rule ID: SV-238218r877377\_rule

STIG ID: UBTU-20-010047

Severity: CAT I

**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

## 4.2.11 Ensure SSH PermitUserEnvironment is disabled (Automated)

### Profile Applicability:

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

### Description:

The `PermitUserEnvironment` option allows users to present environment options to the SSH daemon.

### Rationale:

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has SSH executing trojan'd programs)

### Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permituserenvironment
```

Verify the output matches:

```
permituserenvironment no
```

Run the following command and verify the output:

```
# grep -Pis '^h*PermitUserEnvironment\h+?yes"\?\b' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf
```

Nothing should be returned.

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` are used in your environment, those locations should be checked for the correct configuration as well.

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
PermitUserEnvironment no
```

**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:**

PermitUserEnvironment no

**References:**

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 :: CM-6

**Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238218  
Rule ID: SV-238218r877377\_rule  
STIG ID: UBTU-20-010047  
Severity: CAT I

**MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1021	TA0008	M1042

#### 4.2.12 Ensure SSH IgnoreRhosts is enabled (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

##### Description:

The `IgnoreRhosts` parameter specifies that `.rhosts` and `.shosts` files will not be used in `RhostsRSAAuthentication` or `HostbasedAuthentication`.

##### Rationale:

Setting this parameter forces users to enter a password when authenticating with SSH.

##### Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep ignorerhosts
```

Verify the output matches:

```
ignorerhosts yes
```

Run the following command:

```
# grep -Pis '^h*ignorerhosts\h+?no"?\\b' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf
```

Nothing should be returned.

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or `Match` set statements are used in your environment, those locations should be checked for the correct configuration as well.

##### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` 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)

## 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

#### 4.2.13 Ensure SSH X11 forwarding is disabled (Automated)

##### Profile Applicability:

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

##### Description:

The `X11Forwarding` parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.

##### Rationale:

Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

##### Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i x11forwarding
```

Verify the output matches:

```
x11forwarding no
```

Run the following command:

```
# grep -Pis '^x11forwarding\h+?yes"?\\b' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf
```

Nothing is returned.

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or `Match` set statements are used in your environment, those locations should be checked for the correct configuration as well.

##### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
x11Forwarding 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.

## References:

1. NIST SP 800-53 :: CM-6 b

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238219  
Rule ID: SV-238219r858533\_rule  
STIG ID: UBTU-20-010048  
Severity: CAT I

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

## MITRE ATT&CK Mappings:

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

#### *4.2.14 Ensure only strong Ciphers are used (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

This variable limits the ciphers that SSH can use during communication.

##### **Note:**

- Some organizations may have stricter requirements for approved ciphers.
- Ensure that ciphers used are in compliance with site policy.
- The only "strong" ciphers currently FIPS 140-2 compliant are:
  - 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:

```
# sshd -T -C user=root -C host="$ (hostname)" -C addr="$ (grep $ (hostname) /etc/hosts | awk '{print $1}')" | grep ciphers
```

Verify that output does not contain any of the following weak ciphers:

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
rijndael-cbc@lysator.liu.se
```

## **Remediation:**

Edit the `/etc/ssh/sshd_config` file add/modify the `Ciphers` line to contain a comma separated list of the site approved ciphers above any `Include` entries:

*Example:*

```
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
```

**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:**

Ciphers [chacha20-poly1305@openssh.com](mailto:chacha20-poly1305@openssh.com),[aes128-ctr](mailto:aes128-ctr),[aes192-ctr](mailto:aes192-ctr),[aes256-ctr](mailto:aes256-ctr),[aes128-gcm@openssh.com](mailto:aes128-gcm@openssh.com),[aes256-gcm@openssh.com](mailto:aes256-gcm@openssh.com)

## **References:**

1. <https://nvd.nist.gov/vuln/detail/CVE-2016-2183>
2. <https://www.openssh.com/txt/cbc.adv>
3. <https://nvd.nist.gov/vuln/detail/CVE-2008-5161>
4. <https://www.openssh.com/txt/cbc.adv>
5. SSHD\_CONFIG(5)

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
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

#### *4.2.15 Ensure only strong MAC algorithms are used (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

This variable limits the types of MAC algorithms that SSH can use during communication.

##### **Notes:**

- Some organizations may have stricter requirements for approved MACs.
- Ensure that MACs used are in compliance with site policy.
- The only "strong" MACs currently FIPS 140-2 approved are:
  - hmac-sha2-256
  - hmac-sha2-512

##### **Rationale:**

MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information.

##### **Audit:**

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i "MACs"
```

Verify that output does not contain any of the listed weak MAC algorithms:

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-sha1
hmac-sha1-96
umac-64@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
```

## **Remediation:**

Edit the `/etc/ssh/sshd_config` file and add/modify the MACs line to contain a comma separated list of the site approved MACs above any `Include` entries:

**Example:**

```
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128-etm@openssh.com,umac-128@openssh.com
```

**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:**

```
MACs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
```

## **References:**

1. More information on SSH downgrade attacks can be found here:  
<http://www.mitls.org/pages/attacks/SLOTH>
2. `SSHD_CONFIG(5)`
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>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:**

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1040, T1040.000, T1557, T1557.000	TA0006	M1041

DRAFT

#### *4.2.16 Ensure only strong Key Exchange algorithms are used (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received

##### **Notes:**

- Kex algorithms have a higher preference the earlier they appear in the list
- Some organizations may have stricter requirements for approved Key exchange algorithms
- Ensure that Key exchange algorithms used are in compliance with site policy
- The only Key Exchange Algorithms currently FIPS 140-2 approved are:
  - ecdh-sha2-nistp256
  - ecdh-sha2-nistp384
  - ecdh-sha2-nistp521
  - diffie-hellman-group-exchange-sha256
  - diffie-hellman-group16-sha512
  - diffie-hellman-group18-sha512
  - diffie-hellman-group14-sha256

##### **Rationale:**

Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

## Audit:

Run the following command and verify that output does not contain any of the listed weak Key Exchange algorithms:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep kexalgorithms
```

### Weak Key Exchange Algorithms:

```
diffie-hellman-group1-sha1  
diffie-hellman-group14-sha1  
diffie-hellman-group-exchange-sha1
```

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or `Match` set statements are used in your environment, those locations should be checked for the correct configuration as well.

## Remediation:

Edit the `/etc/ssh/sshd_config` file add/modify the `KexAlgorithms` line to contain a comma separated list of the site approved key exchange algorithms above any `Include` entries:  
*Example:*

```
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
```

**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:

`KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256`

## References:

1. 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, T1557.000	TA0006	M1041

#### *4.2.17 Ensure SSH AllowTcpForwarding is disabled (Automated)*

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

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

SSH port forwarding is a mechanism in SSH for tunneling application ports from the client to the server, or servers to clients. It can be used for adding encryption to legacy applications, going through firewalls, and some system administrators and IT professionals use it for opening backdoors into the internal network from their home machines.

##### **Rationale:**

Leaving port forwarding enabled can expose the organization to security risks and backdoors.

SSH connections are protected with strong encryption. This makes their contents invisible to most deployed network monitoring and traffic filtering solutions. This invisibility carries considerable risk potential if it is used for malicious purposes such as data exfiltration. Cybercriminals or malware could exploit SSH to hide their unauthorized communications, or to exfiltrate stolen data from the target network.

##### **Impact:**

SSH tunnels are widely used in many corporate environments. In some environments the applications themselves may have very limited native support for security. By utilizing tunneling, compliance with SOX, HIPAA, PCI-DSS, and other standards can be achieved without having to modify the applications.

## Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i allowtcpforwarding
```

Verify the output matches:

```
allowtcpforwarding no
```

Run the following command:

```
# grep -Pis '^h*AllowTcpForwarding\h+?yes\b' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf
```

Nothing should be returned.

**Note:** If Include locations besides, or in addition to /etc/ssh/sshd\_config.d/\*.conf and/or Match set statements are used in your environment, those locations should be checked for the correct configuration as well.

## Remediation:

Edit the /etc/ssh/sshd\_config file to set the parameter above any Include entries as follows:

```
AllowTcpForwarding 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:

AllowTcpForwarding yes

## References:

1. <https://www.ssh.com/ssh/tunneling/example>
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
T1048, T1048.002, T1572, T1572.000	TA0008	M1042

#### 4.2.18 Ensure SSH warning banner is configured (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

##### Description:

The `Banner` parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

##### Rationale:

Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

##### Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep banner
```

Verify the output matches:

```
banner /etc/issue.net
```

##### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` 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. 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

#### 4.2.19 Ensure SSH MaxAuthTries is set to 4 or less (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

##### Description:

The `MaxAuthTries` parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the `syslog` file detailing the login failure.

##### Rationale:

Setting the `MaxAuthTries` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

##### Audit:

Run the following command and verify that output `MaxAuthTries` is 4 or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep maxauthtries  
maxauthtries 4
```

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or `Match` set statements are used in your environment, those locations should be checked for the correct configuration as well.

Run the following command and verify that the output:

```
# grep -Pis '^h*maxauthtries\h+?"([5-9]| [1-9] [0-9]+)\b' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf  
  
Nothing is returned
```

##### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
MaxAuthTries 4
```

**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:

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

## 4.2.20 Ensure SSH MaxStartups is configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `MaxStartups` parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.

### Rationale:

To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of `MaxStartups` to protect availability of `sshd` logins and prevent overwhelming the daemon.

### Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i maxstartups
```

Verify that output `MaxStartups` is 10:30:60 or more restrictive:

```
maxstartups 10:30:60
```

Run the following command and verify the output:

```
# grep -Pis '^h*maxstartups\h+”?((([1-9]| [1-9] [0-9] [0-9]+):([0-9]+):([0-9]+))|(([0-9]+):(3[1-9]| [4-9] [0-9]| [1-9] [0-9] [0-9]+):([0-9]+))|(([0-9]+):([0-9]+):(6[1-9]| [7-9] [0-9]| [1-9] [0-9] [0-9]+)))\b' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf
```

Nothing should be returned.

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or `Match` set statements are used in your environment, those locations should be checked for the correct configuration as well.

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter 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

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

**MITRE ATT&CK Mappings:**

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.002	TA0040	

## *4.2.21 Ensure SSH LoginGraceTime is set to one minute or less (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `LoginGraceTime` parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access.

### **Rationale:**

Setting the `LoginGraceTime` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections. While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

### **Audit:**

Run the following command and verify that output `LoginGraceTime` is between 1 and 60 seconds or `1m`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep logingracetime  
logingracetime 60
```

Run the following command and verify the output:

```
# grep -Pis '^h*LoginGraceTime\h+?(0|6[1-9]|7-9[0-9]|1-9[0-9][0-9]+|^1m)\b' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf  
Nothing should be returned
```

**Note:** If Include locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or Match set statements are used in your environment, those locations should be checked for the correct configuration as well.

## **Remediation:**

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
LoginGraceTime 60
```

**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:**

```
LoginGraceTime 120
```

## **References:**

1. [SSHD\\_CONFIG\(5\)](#)
2. [NIST SP 800-53 Rev. 5: CM-6](#)

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

<b>Techniques / Sub-techniques</b>	<b>Tactics</b>	<b>Mitigations</b>
T1110, T1110.001, T1110.003, T1110.004	TA0006	M1036

## 4.2.22 Ensure SSH MaxSessions is set to 10 or less (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `MaxSessions` parameter specifies the maximum number of open sessions permitted from a given connection.

### Rationale:

To protect a system from denial of service due to a large number of concurrent sessions, use the rate limiting function of `MaxSessions` to protect availability of `sshd` logins and prevent overwhelming the daemon.

### Audit:

Run the following command and verify that output `MaxSessions` is 10 or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i maxsessions  
maxsessions 10
```

Run the following command and verify the output:

```
grep -Pis '^h*MaxSessions\h+?(1[1-9]|2[0-9]|1[0-9][0-9]|1[0-9][0-9][0-9]+)\b' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf
```

Nothing should be returned

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or `Match` set statements are used in your environment, those locations should be checked for the correct configuration as well.

### Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
MaxSessions 10
```

**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:

`MaxSessions 10`

**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:**

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.002	TA0040	

DRAFT

## *4.2.23 Ensure SSH Idle Timeout Interval is configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

**Note:** To clarify, the two settings described below 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 commands and verify `ClientAliveInterval` is greater than zero:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep clientaliveinterval
```

*Example output:*

```
clientaliveinterval 15
```

Run the following command and verify `ClientAliveCountMax` is greater than zero:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep clientalivecountmax
```

*Example output:*

```
clientalivecountmax 3
```

Run the following command:

```
# grep -Pis '^h*ClientAliveCountMax\h+?"?0\b' /etc/ssh/sshd_config  
/etc/ssh/sshd_config.d/*.conf
```

Nothing should be returned

**Note:** If `Include` locations besides, or in addition to `/etc/ssh/sshd_config.d/*.conf` and/or `Match` set statements are used in your environment, those locations should be checked for the correct configuration as well.

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameters above any `Include` 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. [https://man.openbsd.org/sshd\\_config](https://man.openbsd.org/sshd_config)
2. 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

#### *4.2.24 Ensure network connections associated with SSH traffic are terminated after a period of inactivity (Automated)*

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

- STIG

##### **Description:**

The operating system must immediately terminate all network connections associated with SSH traffic after a period of inactivity.

##### **Rationale:**

Automatic session termination addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions.

Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on information system use.

This capability is typically reserved for specific Ubuntu operating system functionality where the system owner, data owner, or organization requires additional assurance.

##### **Audit:**

Verify that all network connections associated with SSH traffic automatically terminate after a period of inactivity.

Verify the "ClientAliveCountMax" variable is set in the "/etc/ssh/sshd\_config" file by performing the following command:

```
# grep -i clientalivecountmax /etc/ssh/sshd_config
```

```
ClientAliveCountMax 1
```

If "ClientAliveCountMax" is not set, is not set to "1", or is commented out, this is a finding.

## **Remediation:**

Configure the Ubuntu operating system to automatically terminate inactive SSH sessions after a period of inactivity.

Modify or append the following line in the "/etc/ssh/sshd\_config" file, replacing "[Count]" with a value of 1:

```
ClientAliveCountMax 1
```

Restart the SSH daemon for the changes to take effect:

```
# systemctl restart sshd.service
```

## **References:**

1. NIST SP 800-53 :: MA-4 e

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238212

Rule ID: SV-238212r858521\_rule

STIG ID: UBTU-20-010036

Severity: CAT II

## **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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

#### *4.2.25 Ensure network connections associated with SSH traffic are terminated at the end of the session or 10 minutes of inactivity (Automated)*

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

- STIG

##### **Description:**

The operating system must immediately terminate all network connections associated with SSH traffic at the end of the session or after 10 minutes of inactivity.

##### **Rationale:**

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

##### **Audit:**

Verify that all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity.

Verify the "ClientAliveInterval" variable is set to a value of "600" or less by performing the following command:

```
# grep -i clientalive /etc/ssh/sshd_config  
ClientAliveInterval 600
```

If "ClientAliveInterval" does not exist, is not set to a value of "600" or less in "/etc/ssh/sshd\_config", or is commented out, this is a finding.

## **Remediation:**

Configure the Ubuntu operating system to automatically terminate all network connections associated with SSH traffic at the end of a session or after a 10-minute period of inactivity.

Modify or append the following line in the "/etc/ssh/sshd\_config" file replacing "[Interval]" with a value of "600" or less:

```
ClientAliveInterval 600
```

Restart the SSH daemon for the changes to take effect:

```
# systemctl restart sshd.service
```

## **References:**

1. NIST SP 800-53 :: SC-10

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238213

Rule ID: SV-238213r858523\_rule

STIG ID: UBTU-20-010037

Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.1 Establish and Maintain a Vulnerability Management Process</b> Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

**4.2.26 Ensure Standard Mandatory DoD Notice and Consent Banner displayed before granting any local or remote connection to the system (Manual)**

**Profile Applicability:**

- STIG

**Description:**

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting any local or remote connection to the system.

**Rationale:**

Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Satisfies: SRG-OS-000228-GPOS-00088, SRG-OS-000023-GPOS-00006

## Audit:

Verify the Ubuntu operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the Ubuntu operating system via an SSH logon with the following command:

```
# grep -i banner /etc/ssh/sshd_config  
Banner /etc/issue.net
```

The command will return the banner option along with the name of the file that contains the SSH banner. If the line is commented out, this is a finding.

Verify the specified banner file matches the Standard Mandatory DoD Notice and Consent Banner exactly:

```
# cat /etc/issue.net  
  
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.  
  
By using this IS (which includes any device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.  
  
-At any time, the USG may inspect and seize data stored on this IS.  
  
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.  
  
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.  
  
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."
```

If the banner text does not match the Standard Mandatory DoD Notice and Consent Banner exactly, this is a finding.

## **Remediation:**

Set the parameter Banner in "/etc/ssh/sshd\_config" to point to the "/etc/issue.net" file:

```
# sed -i '/^Banner/d' /etc/ssh/sshd_config  
# sed -i '$aBanner /etc/issue.net' /etc/ssh/sshd_config
```

Either create the file containing the banner or replace the text in the file with the Standard Mandatory DoD Notice and Consent Banner. The DoD required text is:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Restart the SSH daemon for the changes to take effect and then signal the SSH server to reload the configuration file:

```
# systemctl -s SIGHUP kill sshd
```

## **References:**

1. NIST SP 800-53 :: AC-8

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238214  
Rule ID: SV-238214r858525\_rule  
STIG ID: UBTU-20-010038  
Severity: CAT II

## **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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

#### *4.2.27 Ensure only FIPS validated MAC algorithms are used (Automated)*

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

- STIG

##### **Description:**

The Ubuntu operating system must configure the SSH daemon to use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hashes to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.

##### **Rationale:**

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless. Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network.

Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes.

Satisfies: SRG-OS-000424-GPOS-00188, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173

##### **Audit:**

Verify the SSH daemon is configured to only use MACs that employ FIPS 140-2 approved ciphers with the following command:

```
# grep -i macs /etc/ssh/sshd_config
MACs hmac-sha2-512,hmac-sha2-256
```

If any ciphers other than "hmac-sha2-512" or "hmac-sha2-256" are listed, the order differs from the example above, or the returned line is commented out, this is a finding.

## **Remediation:**

Configure the Ubuntu operating system to allow the SSH daemon to only use MACs that employ FIPS 140-2 approved ciphers.

Add the following line (or modify the line to have the required value) to the "/etc/ssh/sshd\_config" file (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

```
MACs hmac-sha2-512,hmac-sha2-256
```

Restart the SSH daemon for the changes to take effect:

```
# systemctl reload sshd.service
```

## **Default Value:**

MACs [umac-64-etm@openssh.com](#),[umac-128-etm@openssh.com](#),[hmac-sha2-256-etm@openssh.com](#),[hmac-sha2-512-etm@openssh.com](#),[hmac-sha1-etm@openssh.com](#),[umac-64@openssh.com](#),[umac-128@openssh.com](#),[hmac-sha2-256](#),[hmac-sha2-512](#),[hmac-sha1](#)

## **References:**

1. SSSH\_CONFIG(5)
2. NIST SP 800-53 :: AC-17
3. NIST SP 800-53 Revision 4 :: SC-8
4. NIST SP 800-53 Revision 4 :: MA-4

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238216  
Rule ID: SV-238216r877465\_rule  
STIG ID: UBTU-20-010043  
Severity: CAT II

Satisfies: SRG-OS-000424-GPOS-00188, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173

## 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.		●	●

#### *4.2.28 Ensure only FIPS validated Ciphers are used (Automated)*

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

- STIG

##### **Description:**

The operating system must configure the SSH daemon to use FIPS 140-2 approved ciphers to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.

##### **Rationale:**

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network.

Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes.

By specifying a cipher list with the order of ciphers being in a "strongest to weakest" orientation, the system will automatically attempt to use the strongest cipher for securing SSH connections.

Satisfies: SRG-OS-000424-GPOS-00188, SRG-OS-000033-GPOS-00014, SRG-OS-000394-GPOS-00174

## Audit:

Verify the SSH daemon is configured to only implement FIPS-approved algorithms by running the following command:

```
# grep -E 'Ciphers' /etc/ssh/sshd_config  
Ciphers aes256-ctr,aes192-ctr, aes128-ctr
```

If any ciphers other than "aes256-ctr", "aes192-ctr", or "aes128-ctr" are listed, the order differs from the example above, the "Ciphers" keyword is missing, or the returned line is commented out, this is a finding.

## Remediation:

Configure the Ubuntu operating system to allow the SSH daemon to only implement FIPS-approved algorithms.

Add the following line (or modify the line to have the required value) to the "/etc/ssh/sshd\_config" file (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

```
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
```

Restart the SSH daemon for the changes to take effect:

```
# systemctl restart sshd.service
```

## Default Value:

Ciphers [chacha20-poly1305@openssh.com](mailto:chacha20-poly1305@openssh.com),[aes128-ctr](mailto:aes128-ctr),[aes192-ctr](mailto:aes192-ctr),[aes256-ctr](mailto:aes256-ctr),[aes128-gcm@openssh.com](mailto:aes128-gcm@openssh.com),[aes256-gcm@openssh.com](mailto:aes256-gcm@openssh.com)

## References:

1. NIST SP 800-53 :: AC-17
2. NIST SP 800-53 Revision 4 :: SC-8
3. NIST SP 800-53 Revision 4 :: MA-4

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238217  
Rule ID: SV-238217r877465\_rule  
STIG ID: UBTU-20-010044  
Severity: CAT II

Satisfies: SRG-OS-000424-GPOS-00188, SRG-OS-000033-GPOS-00014, SRG-OS-000394-GPOS-00174

## 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.		●	●

DRAFT

## *4.2.29 Ensure only FIPS validated Key Exchange algorithms are used (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received

### **Notes:**

- Kex algorithms have a higher preference the earlier they appear in the list
- Some organizations may have stricter requirements for approved Key exchange algorithms
- Ensure that Key exchange algorithms used are in compliance with site policy
- The only Key Exchange Algorithms currently FIPS 140-2 approved are:
  - ecdh-sha2-nistp256
  - ecdh-sha2-nistp384
  - ecdh-sha2-nistp521
  - diffie-hellman-group-exchange-sha256

### **Rationale:**

Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

### **Audit:**

Run the following command and verify that output does not contain any non FIPS validated Key Exchange algorithms:

```
# sshd -T -C user=root -C host="$ (hostname)" -C addr="$ (grep $ (hostname) /etc/hosts | awk '{print $1}')" | grep kexalgorithms
```

Output should be:

```
KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256
```

**Note:** If Include locations besides, or in addition to /etc/ssh/sshd\_config.d/\*.conf and/or Match set statements are used in your environment, those locations should be checked for the correct configuration as well.

## **Remediation:**

Edit the /etc/ssh/sshd\_config file add/modify the KexAlgorithms line to contain a comma separated list of FIPS validated key exchange algorithms above any `Include` entries:

```
KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256
```

**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:**

```
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256
```

## **References:**

1. 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, T1557.000	TA0006	M1041

#### *4.2.30 Ensure X11UseLocalhost is enabled (Automated)*

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

- STIG

##### **Description:**

The operating system SSH daemon must prevent remote hosts from connecting to the proxy display.

##### **Rationale:**

When X11 forwarding is enabled, there may be additional exposure to the server and client displays if the sshd proxy display is configured to listen on the wildcard address. By default, sshd binds the forwarding server to the loopback address and sets the hostname part of the DISPLAY environment variable to localhost. This prevents remote hosts from connecting to the proxy display.

##### **Audit:**

Verify the SSH daemon prevents remote hosts from connecting to the proxy display. Check the SSH X11UseLocalhost setting with the following command:

```
# grep -i x11uselocalhost /etc/ssh/sshd_config  
X11UseLocalhost yes
```

If the "X11UseLocalhost" keyword is set to "no", is missing, or is commented out, this is a finding.

##### **Remediation:**

Configure the SSH daemon to prevent remote hosts from connecting to the proxy display.

Edit the "/etc/ssh/sshd\_config" file to uncomment or add the line for the "X11UseLocalhost" keyword and set its value to "yes" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

```
X11UseLocalhost yes
```

Restart the SSH daemon for the changes to take effect:

```
# systemctl restart sshd.service
```

##### **References:**

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

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238220  
Rule ID: SV-238220r653835\_rule  
STIG ID: UBTU-20-010049  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

## 4.3 Configure privilege escalation

There are various tools which allows a permitted user to execute a command as the superuser or another user, as specified by the security policy.

### **sudo**

[sudo documentation](#)

The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

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

### **pkexec**

[pkexec documentation](#)

`pkexec` allows an authorized user to execute *PROGRAM* as another user. If *username* is not specified, then the program will be executed as the administrative super user, `root`.

### 4.3.1 Ensure sudo is installed (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

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

#### Rationale:

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

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

#### Audit:

Run the following command to verify that either `sudo` or `sudo-ldap` is installed:

```
# dpkg-query -W sudo sudo-ldap > /dev/null 2>&1 && dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n' sudo sudo-ldap | awk '$4=="installed" && $NF=="installed" {print "\n""PASS:\n""Package\n""$1""\n"" is installed"\n}' || echo -e "\nFAIL:\nneither \"sudo\" or\n\"sudo-ldap\" package is installed\n"
```

#### 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-2, 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
T1078, T1078.003	TA0001	

#### 4.3.2 Ensure sudo commands use pty (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

##### Description:

`sudo` can be configured to run only from a pseudo terminal (`pseudo-pty`).

##### Rationale:

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

##### Impact:

**WARNING:** Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

##### Audit:

Verify that `sudo` can only run other commands from a pseudo terminal.

Run the following command:

```
# grep -rPi '^h*Defaults\h+([^\#\n\r]+,) ?use_pty(,\h*\h+\h*)*\h*(#.*)?$$' /etc/sudoers*
```

Verify the output matches:

```
/etc/sudoers:Defaults use_pty
```

##### Remediation:

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

```
Defaults use_pty
```

##### 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)

## 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:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.003, T1548, T1548.003	TA0001, TA0003	M1026, M1038

### 4.3.3 Ensure sudo log file exists (Automated)

#### Profile Applicability:

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

#### 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\s+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)

## 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.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Required for auditd rules

## 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

#### *4.3.4 Ensure only users who need access to security functions are part of sudo group (Manual)*

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

- STIG

##### **Description:**

The operating system must ensure only users who need access to security functions are part of sudo group.

##### **Rationale:**

An isolation boundary provides access control and protects the integrity of the hardware, software, and firmware that perform security functions.

Security functions are the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Operating systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk and address space protections that protect executing code.

Developers and implementers can increase the assurance in security functions by employing well-defined security policy models; structured, disciplined, and rigorous hardware and software development techniques; and sound system/security engineering principles. Implementation may include isolation of memory space and libraries.

The Ubuntu operating system restricts access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

##### **Audit:**

Verify the sudo group has only members who should have access to security functions.

```
# grep ^sudo: /etc/group  
sudo:x:27:foo
```

If the sudo group contains users not needing access to security functions, this is a finding.

## **Remediation:**

Configure the sudo group with only members requiring access to security functions.  
To remove a user from the sudo group, run:

```
# sudo gpasswd -d <username> sudo
```

## **References:**

1. NIST SP 800-53 :: SC-3

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238206  
Rule ID: SV-238206r653793\_rule  
STIG ID: UBTU-20-010012  
Severity: CAT I

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●

#### *4.3.5 Ensure users must provide password for privilege escalation (Automated)*

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

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

##### **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

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238208  
Rule ID: SV-238208r853405\_rule  
STIG ID: UBTU-20-010014  
Severity: CAT II

## **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
T1078, T1548	TA0005	M1026

#### *4.3.6 Ensure re-authentication for privilege escalation is not disabled globally (Automated)*

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

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

##### **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

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238208  
Rule ID: SV-238208r853405\_rule  
STIG ID: UBTU-20-010014  
Severity: CAT II

## **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.	●	●	●

#### *4.3.7 Ensure sudo authentication timeout is configured correctly (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

`sudo` caches used credentials for a default of 15 minutes. This is for ease of use when there are multiple administrative tasks to perform. The timeout can be modified to suit local security policies.

This default is distribution specific. See audit section for further information.

##### **Rationale:**

Setting a timeout value reduces the window of opportunity for unauthorized privileged access to another user.

##### **Audit:**

Ensure that the caching timeout is no more than 15 minutes.

##### **Example:**

```
# grep -roP "timestamp_timeout=\K[0-9]*" /etc/sudoers*
```

If there is no `timestamp_timeout` configured in `/etc/sudoers*` then the default is 15 minutes. This default can be checked with:

```
# sudo -V | grep "Authentication timestamp timeout:"
```

**NOTE:** A value of `-1` means that the timeout is disabled. Depending on the configuration of the `timestamp_type`, this could mean for all terminals / processes of that user and not just that one single terminal session.

##### **Remediation:**

If the currently configured timeout is larger than 15 minutes, edit the file listed in the audit section with `visudo -f <PATH TO FILE>` and modify the entry `timestamp_timeout=` to 15 minutes or less as per your site policy. The value is in minutes. This particular entry may appear on it's own, or on the same line as `env_reset`. See the following two examples:

```
Defaults    env_reset, timestamp_timeout=15
Defaults    timestamp_timeout=15
Defaults    env_reset
```

## References:

1. <https://www.sudo.ws/man/1.9.0/sudoers.man.html>
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.	●	●	●

#### 4.3.8 Ensure access to the su command is restricted (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

##### Description:

The `su` command allows a user to run a command or shell as another user. The program has been superseded by `sudo`, which allows for more granular control over privileged access. Normally, the `su` command can be executed by any user. By uncommenting the `pam_wheel.so` statement in `/etc/pam.d/su`, the `su` command will only allow users in a specific group to execute `su`. This group should be empty to reinforce the use of `sudo` for privileged access.

##### Rationale:

Restricting the use of `su`, and using `sudo` in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The `sudo` utility also provides a better logging and audit mechanism, as it can log each command executed via `sudo`, whereas `su` can only record that a user executed the `su` program.

##### Audit:

Run the following command:

```
# grep -Pi '^auth[ ]+required[ ]+pam_wheel\.so[ ]+group=[^#n\]+[ ]+use_uid\b|group=\H+\b)' /etc/pam.d/su
```

Verify the output matches:

```
auth required pam_wheel.so use_uid group=<group_name>
```

Run the following command and verify that the group specified in `<group_name>` contains no users:

```
# grep <group_name> /etc/group
```

Verify the output does not contain any users in the relevant group:

```
<group_name>:x:<GID>:
```

## **Remediation:**

Create an empty group that will be specified for use of the `su` command. The group should be named according to site policy.

Example:

```
# groupadd sugroup
```

Add the following line to the `/etc/pam.d/su` file, specifying the empty group:

```
auth required pam_wheel.so use_uid group=sugroup
```

## **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, T1548.000	TA0005	M1026

## 4.4 Configure Pluggable Authentication Modules

Pluggable Authentication Modules (PAM) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the `/etc/pam.d` directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

**Note:** The usage of `pam-auth-update`:

- As of this writing, the management of PAM via `pam-auth-update` does not offer all the required functionality implemented by the benchmark. As such, the usage of `pam-auth-update` is not recommended at present.

#### 4.4.1 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

**Note:** The module arguments override the settings in the `/etc/security/pwquality.conf` configuration file.

#### *4.4.1.1 Ensure new and changed passwords use pwquality (Automated)*

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

- STIG

##### **Description:**

The operating system must be configured so that when passwords are changed or new passwords are established, pwquality must be used.

##### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

##### **Audit:**

Verify the Ubuntu operating system has the "libpam-pwquality" package installed by running the following command:

```
# dpkg -l libpam-pwquality  
ii libpam-pwquality:amd64 1.4.0-2 amd64 PAM module to check password strength
```

If "libpam-pwquality" is not installed, this is a finding.

Verify that the operating system uses "pwquality" to enforce the password complexity rules.

Verify the pwquality module is being enforced by the Ubuntu operating system by running the following command:

```
# grep -i enforcing /etc/security/pwquality.conf  
enforcing = 1
```

If the value of "enforcing" is not "1" or the line is commented out, this is a finding. Check for the use of "pwquality" with the following command:

```
# cat /etc/pam.d/common-password | grep requisite | grep pam_pwquality  
password requisite pam_pwquality.so retry=3
```

If no output is returned or the line is commented out, this is a finding.

If the value of "retry" is set to "0" or greater than "3", this is a finding.

## **Remediation:**

Configure the operating system to use "pwquality" to enforce password complexity rules.

Install the "pam\_pwquality" package by using the following command:

```
# apt-get install libpam-pwquality -y
```

Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
enforcing = 1
```

Add the following line to "/etc/pam.d/common-password" (or modify the line to have the required value):

```
password requisite pam_pwquality.so retry=3
```

**Note:** The value of "retry" should be between "1" and "3".

## **References:**

1. NIST SP 800-53 :: CM-6 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238228

Rule ID: SV-238228r653859\_rule

STIG ID: UBTU-20-010057

Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.		●	●

#### *4.4.1.2 Ensure password creation requirements are configured (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The `pam_pwquality.so` module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.

The following options are set in the `/etc/security/pwquality.conf` file:

- Password Length:
  - `minlen = 14` - password must be 14 characters or more
- Password complexity:
  - `minclass = 4` - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

*OR*

- `dcredit = -1` - provide at least one digit
- `ucredit = -1` - provide at least one uppercase character
- `ocredit = -1` - provide at least one special character
- `lcredit = -1` - provide at least one lowercase character

##### **Rationale:**

Strong passwords protect systems from being hacked through brute force methods.

## Audit:

Verify password creation requirements conform to organization policy.

### Password length

Run the following command:

```
# grep '^s*minlen\s*' /etc/security/pwquality.conf
```

Verify the output matches:

```
minlen = 14
```

### Password complexity

#### Option 1

Run the following command:

```
# grep '^s*minclass\s*' /etc/security/pwquality.conf
```

Verify the output matches:

```
minclass = 4
```

#### Option 2

Run the following command:

```
# grep -E '^s*[duol]credit\s*' /etc/security/pwquality.conf
```

Verify the output matches:

```
dcredit = -1  
ucredit = -1  
lcredit = -1  
ocredit = -1
```

### pam\_pwquality.so enabled

Run the following command to verify pam\_pwquality.so is enabled

```
grep -P '^h*password\h+[^#\n\r]+\h+pam_pwquality\.so\b' /etc/pam.d/common-password
```

*Example output:*

password	requisite	pam_pwquality.so retry=3
----------	-----------	--------------------------

## **Remediation:**

The following setting is a recommend example policy. Alter these values to conform to your own organization's password policies.

Run the following command to install the `pam_pwquality` module:

```
# apt install libpam-pwquality
```

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password length to conform to site policy:

```
minlen = 14
```

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password complexity to conform to site policy:

### **Option 1**

```
minclass = 4
```

### **Option 2**

```
dcredit = -1  
ucredit = -1  
ocredit = -1  
lccredit = -1
```

Edit the `/etc/pam.d/common-password` file to include `pam_pwquality.so` and to conform to site policy:

```
password requisite pam_pwquality.so retry=3
```

## **References:**

1. NIST SP 800-53 Rev. 5: IA-5

## **Additional Information:**

Additional module options may be set, recommendation requirements only cover including `try_first_pass` and `minlen` set to 14 or more.

**NOTE:** As of this writing it is not possible to customize the maximum number of retries for the creation of a password within recommended methods. The command `pam-auth-update` is used to manage certain PAM configurations via profiles, such as `/etc/pam.d/common-password`. Making a manual change to this file will cause `pam-auth-update` to overwrite it on the next run and is thus against recommendations.

Alternatively, `pam_pwquality` (via `/etc/security/pwquality.conf`) fully supports the configuration of the maximum number of retries for a password change with the configuration entry `retry = xxx`. The issue is that the template `/usr/share/pam-configs/pwquality` contains `retry=3` which will override any retry setting in `/etc/security/pwquality.conf` as PAM entries takes precedence. This template file should not be modified as any package update will overwrite the change. Thus it is not possible, in any recommended way, to modify password retries.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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	TA0006	M1027

#### *4.4.1.3 Ensure maximum number of same consecutive characters in a password 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 in `/etc/security/pwquality.conf` is set to 3 or less, and not 0:

```
# grep -Pi '^h*maxrepeat\h*=\\h*[1-3]\\b' /etc/security/pwquality.conf  
maxrepeat = 3
```

**Note:** The check is disabled if the value is 0

##### **Remediation:**

Edit or add the following line in `/etc/security/pwquality.conf` to a value of 3 or less and not 0:

```
maxrepeat = 3
```

##### **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.		●	●

#### *4.4.1.4 Ensure the number of changed characters in a new password 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 in `/etc/security/pwquality.conf` is set to 2 or more:

```
# grep -P '^h*difok\h*=\h*([2-9] | [1-9][0-9]+)\b' /etc/security/pwquality.conf  
difok = 2
```

##### **Remediation:**

Edit or add the following line in `/etc/security/pwquality.conf` to a value of 2 or more:

```
difok = 2
```

##### **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.		●	●

#### *4.4.1.5 Ensure preventing the use of dictionary words for passwords is configured (Automated)*

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

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

##### **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 in `/etc/security/pwquality.conf` is not set to 0:

```
# grep -Pi '^h*dictcheck\h*=\h*[^0]' /etc/security/pwquality.conf
dictcheck = 1
```

##### **Remediation:**

Edit or add the following line in `/etc/security/pwquality.conf` to a value of 1:

```
dictcheck = 1
```

##### **Default Value:**

`dictcheck = 1`

##### **References:**

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

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238227  
Rule ID: SV-238227r653856\_rule  
STIG ID: UBTU-20-010056  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●

#### *4.4.1.6 Ensure password includes at least one upper-case character (Automated)*

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

- STIG

##### **Description:**

The operating system must enforce password complexity by requiring that at least one upper-case character be used.

##### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

##### **Audit:**

Verify the Ubuntu operating system enforces password complexity by requiring that at least one upper-case character be used.

Determine if the field "ucredit" is set in the "/etc/security/pwquality.conf" file with the following command:

```
# grep -i "ucredit" /etc/security/pwquality.conf  
ucredit=-1
```

If the "ucredit" parameter is greater than "-1" or is commented out, this is a finding.

##### **Remediation:**

Add or update the "/etc/security/pwquality.conf" file to contain the "ucredit" parameter:

```
ucredit=-1
```

##### **References:**

1. NIST SP 800-53 :: IA-5

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238221  
Rule ID: SV-238221r653838\_rule  
STIG ID: UBTU-20-010050  
Severity: CAT III

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●

#### *4.4.1.7 Ensure password includes at least one lower-case character (Automated)*

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

- STIG

##### **Description:**

The operating system must enforce password complexity by requiring that at least one lower-case character be used.

##### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

##### **Audit:**

Verify the Ubuntu operating system enforces password complexity by requiring that at least one lower-case character be used.

Determine if the field "lcredit" is set in the "/etc/security/pwquality.conf" file with the following command:

```
# grep -i "lcredit" /etc/security/pwquality.conf  
lcredit=-1
```

If the "lcredit" parameter is greater than "-1" or is commented out, this is a finding.

##### **Remediation:**

Add or update the "/etc/security/pwquality.conf" file to contain the "lcredit" parameter:

```
lcredit=-1
```

##### **References:**

1. NIST SP 800-53 :: IA-5

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238222  
Rule ID: SV-238222r653841\_rule  
STIG ID: UBTU-20-010051  
Severity: CAT III

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●

#### *4.4.1.8 Ensure password includes at least one numeric character (Automated)*

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

- STIG

##### **Description:**

The operating system must enforce password complexity by requiring that at least one numeric character be used.

##### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

##### **Audit:**

Verify the Ubuntu operating system enforces password complexity by requiring that at least one numeric character be used.

Determine if the field "dcredit" is set in the "/etc/security/pwquality.conf" file with the following command:

```
# grep -i "dcredit" /etc/security/pwquality.conf  
dcredit=-1
```

If the "dcredit" parameter is greater than "-1" or is commented out, this is a finding.

##### **Remediation:**

Configure the Ubuntu operating system to enforce password complexity by requiring that at least one numeric character be used.

Add or update the "/etc/security/pwquality.conf" file to contain the "dcredit" parameter:

```
dcredit=-1
```

##### **References:**

1. NIST SP 800-53 :: IA-5

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238223

Rule ID: SV-238223r653844\_rule

STIG ID: UBTU-20-010052

Severity: CAT III

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●

#### *4.4.1.9 Ensure password includes at least one special character (Automated)*

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

- STIG

##### **Description:**

The operating system must enforce password complexity by requiring that at least one special character be used.

##### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity or strength is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor in determining how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ # \$ % ^ \*.

##### **Audit:**

Determine if the field "ocredit" is set in the "/etc/security/pwquality.conf" file with the following command:

```
# grep -i "ocredit" /etc/security/pwquality.conf  
ocredit=-1
```

If the "ocredit" parameter is greater than "-1" or is commented out, this is a finding.

##### **Remediation:**

Configure the Ubuntu operating system to enforce password complexity by requiring that at least one special character be used.

Add or update the following line in the "/etc/security/pwquality.conf" file to include the "ocredit=-1" parameter:

```
ocredit=-1
```

##### **References:**

1. NIST SP 800-53 :: IA-5

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238226  
Rule ID: SV-238226r653853\_rule  
STIG ID: UBTU-20-010055  
Severity: CAT III

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●

#### *4.4.1.10 Ensure change of at least 8 characters when passwords are changed (Automated)*

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

- STIG

##### **Description:**

The operating system must require the change of at least 8 characters when passwords are changed.

##### **Rationale:**

If the operating system allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. In other words, characters may be the same within the two passwords; however, the positions of the like characters must be different.

If the password length is an odd number then number of changed characters must be rounded up. For example, a password length of 15 characters must require the change of at least 8 characters.

##### **Audit:**

Verify the Ubuntu operating system requires the change of at least eight characters when passwords are changed.

Determine if the field "difok" is set in the "/etc/security/pwquality.conf" file with the following command:

```
# grep -i "difok" /etc/security/pwquality.conf  
difok=8
```

If the "difok" parameter is less than "8" or is commented out, this is a finding.

##### **Remediation:**

Configure the Ubuntu operating system to require the change of at least eight characters when passwords are changed.

Add or update the "/etc/security/pwquality.conf" file to include the "difok=8" parameter:

```
difok=8
```

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238224  
Rule ID: SV-238224r653847\_rule  
STIG ID: UBTU-20-010053  
Severity: CAT III

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●

#### *4.4.1.11 Ensure password is at least 15 characters (Automated)*

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

- STIG

##### **Description:**

The operating system must enforce a minimum 15-character password length.

##### **Rationale:**

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

##### **Audit:**

Verify the pwquality configuration file enforces a minimum 15-character password length by running the following command:

```
# grep -i ^minlen /etc/security/pwquality.conf  
minlen=15
```

If "minlen" parameter value is not "15" or higher or is commented out, this is a finding.

##### **Remediation:**

Configure the Ubuntu operating system to enforce a minimum 15-character password length.

Add or modify the "minlen" parameter value to the "/etc/security/pwquality.conf" file:

```
minlen=15
```

##### **References:**

1. NIST SP 800-53 :: IA-5

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238225

Rule ID: SV-238225r832942\_rule

STIG ID: UBTU-20-010054

Severity: CAT II

## **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.	●	●	●

## 4.4.2 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.
- conf=</path/to/config-file> - Use another configuration file instead of the default /etc/security/pwhistory.conf.

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
```

The options for configuring the module behavior are described in the pwhistory.conf(5) manual page. The options specified on the module command line override the values from the configuration file.

`pwhistory.conf` provides a way to configure the default settings for saving the last passwords for each user. This file is read by the `pam_pwhistory` module and is the preferred method over configuring `pam_pwhistory` directly.

The file has a very simple name = value format with possible comments starting with # character. The whitespace at the beginning of line, end of line, and around the = sign is ignored.

Options:

- `debug` - Turns on debugging via `syslog(3)`.
- `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.
- `file=</path/filename>` - Store password history in file </path/filename> rather than the default location. The default location is `/etc/security/opasswd`.

#### 4.4.2.1 Ensure password reuse is limited (Automated)

##### Profile Applicability:

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

##### Description:

The `/etc/security/opasswd` file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

##### Rationale:

Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password.

##### Audit:

Run the following command to verify the following in `/etc/pam.d/common-password`:

- The `pam_unix.so` line includes `use_authok`
- The `pam_pwhistory.so` line includes `remember=` and a value no less than 5
- The `pam_pwhistory.so` line occurs before the `pam_unix.so` line, after the `pam_pwquality.so` line, and includes `use_authok`

```
# grep -P --  
'^h*password\h+([^\#\n\r]+\.h+)?(pam_pwhistory\.so|pam_unix\.so|pam_pwquality\.so)\b' /etc/pam.d/common-password
```

##### Example output:

<code>password      requisite</code>	<code>pam_pwquality.so</code>
<code>password      required</code>	<code>pam_pwhistory.so    remember=5</code>
<code>use_authok</code>	
<code>password      [success=1 default=ignore]</code>	<code>pam_unix.so        obscure</code>
<code>sha512      use_authok</code>	

## Remediation:

**NOTE:** Pay special attention to the configuration. Incorrect configuration can cause system lock outs or unexpected behavior. This is example configuration. Your configuration may differ based on previous changes to the files.

Edit the `/etc/pam.d/common-password` file to include:

- `password required pam_pwhistory.so remember=5 use_authtok`
- `use_authtok` on the `pam_unix.so` line

### Example:

```
password      requisite          pam_pwquality.so
password      required          pam_pwhistory.so   remember=5
use_authtok
password      [success=1 default=ignore]    pam_unix.so      obscure
sha512  use_authtok
```

## References:

1. [https://manpages.ubuntu.com/manpages/focal/man8/pam\\_pwhistory.8.html](https://manpages.ubuntu.com/manpages/focal/man8/pam_pwhistory.8.html)
2. <https://bugs.launchpad.net/ubuntu/+source/pam/+bug/1989731>
3. NIST SP 800-53 Rev. 5: AC-2, IA-5

## Additional Information:

Changes only apply to accounts configured on the local system.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238234  
Rule ID: SV-238234r832945\_rule  
STIG ID: UBTU-20-010070  
Severity: CAT III

## 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	TA0005	M1028

DRAFT

#### 4.4.3 Configure pam\_faillock module

faillock.conf provides a way to configure the default settings for locking the user after multiple failed authentication attempts. This file is read by the pam\_faillock module and is the preferred method over configuring pam\_faillock directly.

The file has a very simple name = value format with possible comments starting with # character. The whitespace at the beginning of line, end of line, and around the = sign is ignored.

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.

*Example etc/security/faillock.conf file:*

```
deny=5  
unlock_time=900  
even_deny_root
```

DRAFT

#### *4.4.3.1 Ensure lockout for failed password attempts is configured (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Lock out users after  $n$  unsuccessful consecutive login attempts. The first sets of changes are made to the common PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM.

All configuration of `faillock` is located in `/etc/security/faillock.conf` and well commented.

- `deny` - Deny access if the number of consecutive authentication failures for this user during the recent interval exceeds  $n$  tries.
- `fail_interval` - The length of the interval, in seconds, during which the consecutive authentication failures must happen for the user account to be locked out
- `unlock_time` - 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` command.

Set the lockout number and unlock time in accordance with local site policy.

##### **Rationale:**

Locking out user IDs after  $n$  unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

##### **Impact:**

It is critical to test and validate any PAM changes before deploying. Any misconfiguration could cause the system to be inaccessible.

## Audit:

Verify password lockouts are configured. These settings are commonly configured with the `pam_faillock.so` module found in `/etc/pam.d/common-auth` and `/etc/pam.d/common-account`.

### Common auth

Run the following command to verify `pam_faillock.so` is configured in `/etc/pam.d/common-auth`:

```
# grep "pam_faillock.so" /etc/pam.d/common-auth
```

Verify the output includes the three `pam_faillock.so` lines:

*Example output:*

auth required	pam_faillock.so preauth
auth [default=die]	pam_faillock.so authfail
auth sufficient	pam_faillock.so authsucc

### Common account

Run the following command to verify `pam_faillock.so` is configured in `/etc/pam.d/common-account`:

```
# grep "pam_faillock.so" /etc/pam.d/common-account
```

Verify the output matches:

account required	pam_faillock.so
------------------	-----------------

### Fail lock configuration

Run the following command to verify `deny`, `fail_interval`, and `unlock_time` are configured in `/etc/security/faillock.conf`:

```
awk '/^ *deny */\n ||/^ *fail_interval */\n ||/^ *unlock_time */' /etc/security/faillock.conf
```

Verify the output:

- `deny` is not greater than 4
- `fail_interval` is no greater than 900
- `unlock_time` is 0, or greater than or equal to 600
- Settings follow local site policy

*Example:*

```
deny = 4\nfail_interval = 900\nunlock_time = 600
```

## **Remediation:**

**NOTE:** Pay special attention to the configuration. Incorrect configuration can cause system lock outs. This is example configuration. Your configuration may differ based on previous changes to the files.

### **Common auth**

Edit `/etc/pam.d/common-auth` and ensure that `faillock` is configured.

**Note:** It is critical to understand each line and the relevant arguments for successful implementation. The order of these entries is very specific. The `pam_faillock.so` lines surround the `pam_unix.so` line. **The comment "Added to enable faillock" is shown to highlight the additional lines and their order in the file.**

```
# here are the per-package modules (the "Primary" block)
auth required pam_faillock.so preauth # Added to
enable faillock
auth [success=1 default=ignore] pam_unix.so
auth [default=die] pam_faillock.so authfail # Added to
enable faillock
auth sufficient pam_faillock.so authsucc # Added to
enable faillock
# here's the fallback if no module succeeds
auth requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth required pam_permit.so
```

### **Common account**

Edit `/etc/pam.d/common-account` and **ensure that the following stanza is at the end of the file.**

```
account required pam_faillock.so
```

### **Fail lock configuration**

Edit `/etc/security/faillock.conf` and configure it per your site policy.

*Example:*

```
deny = 4
fail_interval = 900
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 `/usr/sbin/faillock --user username --reset`. This command sets the failed count to 0, effectively unlocking the user.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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

#### *4.4.3.2 Ensure lockout for three or more failed password attempts is configured (Automated)*

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

- STIG

##### **Description:**

Lock out users after  $n$  unsuccessful consecutive login attempts. The first sets of changes are made to the common PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM.

All configuration of `faillock` is located in `/etc/security/faillock.conf` and well commented.

- `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.
- `deny` - Deny access if the number of consecutive authentication failures for this user during the recent interval exceeds  $n$  tries.
- `fail_interval` - The length of the interval, in seconds, during which the consecutive authentication failures must happen for the user account to be locked out
- `unlock_time` - 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` command.

Set the lockout number and unlock time in accordance with local site policy.

##### **Rationale:**

Locking out user IDs after  $n$  unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

##### **Impact:**

It is critical to test and validate any PAM changes before deploying. Any misconfiguration could cause the system to be inaccessible.

## Audit:

Verify password lockouts are configured. These settings are commonly configured with the `pam_faillock.so` module found in `/etc/pam.d/common-auth` and `/etc/pam.d/common-account`.

### Common auth

Run the following command to verify `pam_faillock.so` is configured in `/etc/pam.d/common-auth`:

```
# grep "pam_faillock.so" /etc/pam.d/common-auth
```

Verify the output includes the three `pam_faillock.so` lines:

*Example output:*

```
auth    required          pam_faillock.so preauth
auth    [default=die]    pam_faillock.so authfail
auth    sufficient       pam_faillock.so authsucc
```

### Common account

Run the following command to verify `pam_faillock.so` is configured in `/etc/pam.d/common-account`:

```
# grep "pam_faillock.so" /etc/pam.d/common-account
```

Verify the output matches:

```
account  required      pam_faillock.so
```

## Fail lock configuration

Run the following command to verify `deny`, `fail_interval`, and `unlock_time` are configured in `/etc/security/faillock.conf`:

```
awk '/^ *audit */\
||/^ *silent */\
||/^ *deny *=/\
||/^ *fail_interval *=/\
||/^ *unlock_time *=/' /etc/security/faillock.conf
```

Verify the output:

- audit exists
- silent exists
- deny is no greater than 3
- fail\_interval is no greater than 900
- unlock\_time is 0

*Example:*

```
audit
silent
deny = 3
fail_interval = 900
unlock_time = 0
```

## **Remediation:**

**Note:** Pay special attention to the configuration. Incorrect configuration can cause system lock outs. This is example configuration. Your configuration may differ based on previous changes to the files.

### **Common auth**

Edit `/etc/pam.d/common-auth` and ensure that `faillock` is configured.

**Note:** It is critical to understand each line and the relevant arguments for successful implementation. The order of these entries is very specific. The `pam_faillock.so` lines surround the `pam_unix.so` line. **The comment "Added to enable faillock" is shown to highlight the additional lines and their order in the file.**

```
# here are the per-package modules (the "Primary" block)
auth required pam_faillock.so preauth # Added to
enable faillock
auth [success=1 default=ignore] pam_unix.so
auth [default=die] pam_faillock.so authfail # Added to
enable faillock
auth sufficient pam_faillock.so authsucc # Added to
enable faillock
# here's the fallback if no module succeeds
auth requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth required pam_permit.so
```

### **Common account**

Edit `/etc/pam.d/common-account` and **ensure that the following stanza is at the end of the file.**

```
account required pam_faillock.so
```

### **Faillock configuration**

Edit `/etc/security/faillock.conf` and edit or add the following lines:

```
audit
silent
deny = 3
fail_interval = 900
unlock_time = 0
```

## **References:**

1. FAILLOCK.CONF(5)
2. NIST SP 800-53 :: AC-7 a

## **Additional Information:**

If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_faillock.so` module, the user can be unlocked by issuing the command `/usr/sbin/faillock --user username --reset`. This command sets the failed count to 0, effectively unlocking the user.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238235  
Rule ID: SV-238235r853414\_rule  
STIG ID: UBTU-20-010072  
Severity: CAT III

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

## **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

#### **4.4.4 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.

DRAFT

#### *4.4.4.1 Ensure strong password hashing algorithm is configured (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Hash functions behave as one-way functions by using mathematical operations that are extremely difficult and cumbersome to revert

When a user is created, the password is run through a one-way hashing algorithm before being stored. When the user logs in, the password sent is run through the same one-way hashing algorithm and compared to the hash connected with the provided username. If the hashed password and the stored hash match, the login is valid.

##### **Rationale:**

The `SHA512` hashing algorithm provides stronger hashing than previous available algorithms like `MD5`, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

##### **Audit:**

Run the following command to verify that `pam_unix.so` includes `sha512` in `/etc/pam.d/common-password`:

```
# grep -Pi -- '^h*password\h+[^#\n\r]+\h+pam_unix.so([^\#\n\r]+\h+)?(sha512|yescrypt)\b' /etc/pam.d/common-password
```

##### *Example Output*

```
password [success=1 default=ignore] pam_unix.so obscure sha512  
use_authtok
```

Run the following command to verify that `ENCRYPT_METHOD` is set to `SHA512` in `/etc/login.defs`:

```
# grep -Pi -- '^h*ENCRYPT_METHOD\h+?"?(sha512|yescrypt)\b' /etc/login.defs
```

Verify the output matches:

```
ENCRYPT_METHOD SHA512
```

## **Remediation:**

### **Note:**

- Pay special attention to the configuration. Incorrect configuration can cause system lock outs.
- This is an example configuration. Your configuration may differ based on previous changes to the files.
- The encryption method on the password success line for `pam_unix.so` and the `ENCRYPT_METHOD` line in `/etc/login.defs` should match.

**Edit the `/etc/pam.d/common-password` file and ensure that `sha512` is included and the `pam_unix.so` success line:**

**Example:**

```
password [success=1 default=ignore] pam_unix.so obscure sha512  
use_authtok
```

**Edit `/etc/login.defs` and ensure that `ENCRYPT_METHOD` is set to `SHA512`.**

```
ENCRYPT_METHOD SHA512
```

### **Default Value:**

`sha512`

### **References:**

1. NIST SP 800-53 Rev. 5: IA-5, SC-28

### **Additional Information:**

Additional module options may be set, recommendation only covers those listed here.

`yescrypt` has been included in the audit commands. This hashing algorithm is not currently supported, but it will be acceptable as an alternative to `sha512` if future updates enable its support.

## 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

#### *4.4.4.2 Ensure pam modules do not include nullok (Automated)*

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

- STIG

##### **Description:**

The operating system must not allow accounts configured with blank or null passwords

##### **Rationale:**

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments

##### **Audit:**

Run the following command to verify that pam modules do not include the `nullok` argument in `/etc/pam.d/common-password`:

```
# grep -Psi '^h*([^\#\n\r]+\h+)?nullok\b' /etc/pam.d/common-password
```

Nothing should be returned

##### **Remediation:**

Edit the `/etc/pam.d/common-password` file and ensure any occurrence of `nullok` is removed from the pam modules listed:

*Example* `/etc/pam.d/common-password` file

password	requisite	pam_pwquality.so
password	requisite	pam_pwhistory.so use_authok
password	[success=1 default=ignore]	pam_unix.so obscure sha512
use_authok		
password	requisite	pam_deny.so
password	required	pam_permit.so

##### **References:**

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

## 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.		●	●

#### 4.4.5 Configure System Security Services

sssd.conf - the configuration file for SSSD

File format: - The file has an ini-style syntax and consists of sections and parameters. A section begins with the name of the section in square brackets and continues until the next section begins. An example of section with single and multi-valued parameters:

```
[section]
key = value
key2 = value2,value3
```

#### *4.4.5.1 Ensure PAM prohibits the use of cached authentications after one day (Automated)*

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

- STIG

##### **Description:**

The operating system must be configured such that Pluggable Authentication Module (PAM) prohibits the use of cached authentications after one day.

##### **Rationale:**

If cached authentication information is out-of-date, the validity of the authentication information may be questionable.

##### **Audit:**

If smart card authentication is not being used on the system, this is Not Applicable. Verify that PAM prohibits the use of cached authentications after one day with the following command:

```
# grep offline_credentials_expiration /etc/sssd/sssd.conf  
/etc/sssd/conf.d/*.conf  
  
offline_credentials_expiration = 1
```

If "offline\_credentials\_expiration" is not set to a value of "1" in "/etc/sssd/sssd.conf" or in a file with a name ending in .conf in the "/etc/sssd/conf.d/" directory, this is a finding.

##### **Remediation:**

Configure PAM to prohibit the use of cached authentications after one day. Add or change the following line in "/etc/sssd/sssd.conf" just below the line "[pam]":

```
offline_credentials_expiration = 1
```

**Note:** It is valid for this configuration to be in a file with a name that ends with ".conf" and does not begin with a "." in the "/etc/sssd/conf.d/" directory instead of the "/etc/sssd/sssd.conf" file.

##### **References:**

1. NIST SP 800-53 Revision 5 :: IA-5 (13)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238362  
Rule ID: SV-238362r654261\_rule  
STIG ID: UBTU-20-010441  
Severity: CAT III

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

#### **4.4.6 Configure pam\_pkcs11 module**

The `pam_pkcs11` module allows a X.509 certificate based user login. The certificate and its dedicated private key are thereby accessed by means of an appropriate PKCS#11 module. For the verification of the users' certificates, locally stored CA certificates as well as either online or locally accessible CRLs are used

DRAFT

#### *4.4.6.1 Ensure the libpam-pkcs11 package is installed (Automated)*

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

- STIG

##### **Description:**

The operating system must implement multifactor authentication for remote access to privileged accounts in such a way that one of the factors is provided by a device separate from the system gaining access.

##### **Rationale:**

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

##### **Audit:**

Verify the Ubuntu operating system has the packages required for multifactor authentication installed with the following commands:

```
# dpkg -l | grep libpam-pkcs11
ii libpam-pkcs11 0.6.8-4 amd64 Fully featured PAM module for using PKCS#11
smart cards
```

If the "libpam-pkcs11" package is not installed, this is a finding.

## **Remediation:**

Configure the Ubuntu operating system to implement multifactor authentication by installing the required packages.

Install the "libpam-pkcs11" package on the system with the following command:

```
# apt install libpam-pkcs11
```

## **References:**

1. NIST SP 800-53 Revision 4 :: IA-2

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238230  
Rule ID: SV-238230r853410\_rule  
STIG ID: UBTU-20-010063  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.4 Require MFA for Remote Network Access</b> Require MFA for remote network access.	●	●	●
v8	<b>6.5 Require MFA for Administrative Access</b> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	<b>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

#### *4.4.6.2 Ensure the opensc-pkcs11 is installed (Automated)*

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

- STIG

##### **Description:**

The operating system must accept Personal Identity Verification (PIV) credentials.

##### **Rationale:**

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under Homeland Security Presidential Directive (HSPD) 12, as well as making the CAC a primary component of layered protection for national security systems.

##### **Audit:**

Verify the Ubuntu operating system accepts PIV credentials.

Verify the "opensc-pkcs11" package is installed on the system with the following command:

```
# dpkg -l | grep opensc-pkcs11  
ii opensc-pkcs11:amd64 0.15.0-1Ubuntu1 amd64 Smart card utilities with  
support for PKCS#15 compatible cards
```

If the "opensc-pkcs11" package is not installed, this is a finding.

##### **Remediation:**

Configure the Ubuntu operating system to accept PIV credentials.

Install the "opensc-pkcs11" package using the following command:

```
# apt-get install opensc-pkcs11
```

##### **References:**

1. NIST SP 800-53 Revision 4 :: IA-2

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238231  
Rule ID: SV-238231r853411\_rule  
STIG ID: UBTU-20-010064  
Severity: CAT II

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>6.4 Require MFA for Remote Network Access</b> Require MFA for remote network access.	●	●	●
v8	<b>6.5 Require MFA for Administrative Access</b> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	<b>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

#### *4.4.6.3 Ensure authenticated identity is mapped to the user or group account for PKI-based authentication (Automated)*

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

- STIG

##### **Description:**

The operating system must map the authenticated identity to the user or group account for PKI-based authentication.

##### **Rationale:**

Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

##### **Audit:**

Verify that "use\_mappers" is set to "pwent" in "/etc/pam\_pkcs11/pam\_pkcs11.conf" file:

```
# grep ^use_mappers /etc/pam_pkcs11/pam_pkcs11.conf  
use_mappers = pwent
```

If "use\_mappers" is not found or the list does not contain "pwent" this is a finding.

##### **Remediation:**

Set "use\_mappers=pwent" in "/etc/pam\_pkcs11/pam\_pkcs11.conf" or, if there is already a comma-separated list of mappers, add it to the list, separated by comma, and before the null mapper.

If the system is missing an "/etc/pam\_pkcs11/" directory and an "/etc/pam\_pkcs11/pam\_pkcs11.conf", find an example to copy into place and modify accordingly at "/usr/share/doc/libpam-pkcs11/examples/pam\_pkcs11.conf.example.gz".

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238201  
Rule ID: SV-238201r832933\_rule  
STIG ID: UBTU-20-010006  
Severity: CAT I

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>6.4 Require MFA for Remote Network Access</b> Require MFA for remote network access.	●	●	●
v8	<b>6.5 Require MFA for Administrative Access</b> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	<b>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

#### *4.4.6.4 Ensure smart card logins for multifactor authentication for local and network access (Automated)*

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

- STIG

##### **Description:**

The operating system must implement smart card logins for multifactor authentication for local and network access to privileged and non-privileged accounts.

##### **Rationale:**

Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased.

Multifactor authentication requires using two or more factors to achieve authentication.

Factors include:

1. something a user knows (e.g., password/PIN);
2. something a user has (e.g., cryptographic identification device, token); and
3. something a user is (e.g., biometric).

A privileged account is defined as an information system account with authorizations of a privileged user.

Network access is defined as access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the internet).

The DoD CAC with DoD-approved PKI is an example of multifactor authentication.

Satisfies: SRG-OS-000105-GPOS-00052, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055

## Audit:

Verify the Ubuntu operating system has the packages required for multifactor authentication installed with the following commands:

```
# dpkg -l | grep libpam-pkcs11  
ii libpam-pkcs11 0.6.8-4 amd64 Fully featured PAM module for using PKCS#11  
smart cards
```

If the "libpam-pkcs11" package is not installed, this is a finding.

Verify the sshd daemon allows public key authentication with the following,

```
# grep ^Pubkeyauthentication /etc/ssh/sshd_config  
  
PubkeyAuthentication yes
```

If this option is set to "no" or is missing, this is a finding.

## Remediation:

Configure the Ubuntu operating system to use multifactor authentication for network access to accounts.

Add or update "pam\_pkcs11.so" in "/etc/pam.d/common-auth" to match the following line:

```
auth [success=2 default=ignore] pam_pkcs11.so
```

Set the sshd option "PubkeyAuthentication yes" in the "/etc/ssh/sshd\_config" file.

## References:

1. NIST SP 800-53 :: IA-2 (1)
2. NIST SP 800-53 :: IA-2 (2)
3. NIST SP 800-53 :: IA-2 (3)
4. NIST SP 800-53 :: IA-2 (4)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238210  
Rule ID: SV-238210r653805\_rule  
STIG ID: UBTU-20-010033  
Severity: CAT II

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>6.4 Require MFA for Remote Network Access</b> Require MFA for remote network access.	●	●	●
v8	<b>6.5 Require MFA for Administrative Access</b> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	<b>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

#### *4.4.6.5 Ensure certificates are validated by constructing a certification path to an accepted trust anchor (Automated)*

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

- STIG

##### **Description:**

The Ubuntu operating system, for PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

##### **Rationale:**

Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a Certification Authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

This requirement verifies that a certification path to an accepted trust anchor is used for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses. Validation of the certificate status information is out of scope for this requirement.

##### **Audit:**

Verify the Ubuntu operating system, for PKI-based authentication, has valid certificates by constructing a certification path to an accepted trust anchor.

Determine which pkcs11 module is being used via the "use\_pkcs11\_module" in "/etc/pam\_pkcs11/pam\_pkcs11.conf" and then ensure "ca" is enabled in "cert\_policy" with the following command:

```
# grep use_pkcs11_module /etc/pam_pkcs11/pam_pkcs11.conf | awk  
'/pkcs11_module opensc {/,/}/' /etc/pam_pkcs11/pam_pkcs11.conf | grep  
cert_policy | grep ca  
  
cert_policy = ca,signature,ocsp_on;
```

If "cert\_policy" is not set to "ca" or the line is commented out, this is a finding.

## **Remediation:**

Configure the Ubuntu operating system, for PKI-based authentication, to validate certificates by constructing a certification path to an accepted trust anchor.

Determine which pkcs11 module is being used via the "use\_pkcs11\_module" in "/etc/pam\_pkcs11/pam\_pkcs11.conf" and ensure "ca" is enabled in "cert\_policy".

Add or update the "cert\_policy" to ensure "ca" is enabled:

```
cert_policy = ca,signature,ocsp_on;
```

If the system is missing an "/etc/pam\_pkcs11/" directory and an

"/etc/pam\_pkcs11/pam\_pkcs11.conf", find an example to copy into place and modify accordingly at "/usr/share/doc/libpam-pkcs11/examples/pam\_pkcs11.conf.example.gz".

## **References:**

1. NIST SP 800-53 :: IA-5

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238229

Rule ID: SV-238229r653862\_rule

STIG ID: UBTU-20-010060

Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.4 Require MFA for Remote Network Access</b> Require MFA for remote network access.	●	●	●
v8	<b>6.5 Require MFA for Administrative Access</b> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	<b>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

#### *4.4.6.6 Ensure Personal Identity Verification credentials are electronically verified (Automated)*

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

- STIG

##### **Description:**

The operating system must electronically verify Personal Identity Verification (PIV) credentials.

##### **Rationale:**

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under Homeland Security Presidential Directive (HSPD) 12, as well as making the CAC a primary component of layered protection for national security systems.

##### **Audit:**

Verify the Ubuntu operating system electronically verifies PIV credentials.

Verify that certificate status checking for multifactor authentication is implemented with the following command:

```
# sudo grep use_pkcs11_module /etc/pam_pkcs11/pam_pkcs11.conf | awk  
'/pkcs11_module opensc {/,/,}/' /etc/pam_pkcs11/pam_pkcs11.conf | grep  
cert_policy | grep ocsp_on  
  
cert_policy = ca,signature,ocsp_on;
```

If "cert\_policy" is not set to "ocsp\_on", or the line is commented out, this is a finding.

##### **Remediation:**

Configure the Ubuntu operating system to do certificate status checking for multifactor authentication.

Modify all of the cert\_policy lines in /etc/pam\_pkcs11/pam\_pkcs11.conf to include ocsp\_on.

##### **References:**

1. NIST SP 800-53 Revision 4 :: IA-2

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238232

Rule ID: SV-238232r853412\_rule

STIG ID: UBTU-20-010065

Severity: CAT II

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>6.4 Require MFA for Remote Network Access</b> Require MFA for remote network access.	●	●	●
v8	<b>6.5 Require MFA for Administrative Access</b> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	<b>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

#### *4.4.6.7 Ensure PKI local cache of revocation data (Automated)*

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

- STIG

##### **Description:**

The operating system for PKI-based authentication, must implement a local cache of revocation data in case of the inability to access revocation information via the network.

##### **Rationale:**

Without configuring a local cache of revocation data, there is the potential to allow access to users who are no longer authorized (users with revoked certificates).

##### **Audit:**

Verify the Ubuntu operating system, for PKI-based authentication, uses local revocation data when unable to access it from the network.

Verify that "crl\_offline" or "crl\_auto" is part of the "cert\_policy" definition in "/etc/pam\_pkcs11/pam\_pkcs11.conf" using the following command:

```
# grep cert_policy /etc/pam_pkcs11/pam_pkcs11.conf | grep -E --  
'crl_auto|crl_offline'  
  
cert_policy = ca,signature,ocsp_on,crl_auto;
```

If "cert\_policy" is not set to include "crl\_auto" or "crl\_offline", this is a finding.

##### **Remediation:**

Configure the Ubuntu operating system, for PKI-based authentication, to use local revocation data when unable to access the network to obtain it remotely.

Add or update the "cert\_policy" option in /etc/pam\_pkcs11/pam\_pkcs11.conf to include crl\_auto or crl\_offline.

```
cert_policy = ca,signature,ocsp_on, crl_auto;
```

If the system is missing an "/etc/pam\_pkcs11/" directory and an "/etc/pam\_pkcs11/pam\_pkcs11.conf", find an example to copy into place and modify accordingly at "/usr/share/doc/libpam-pkcs11/examples/pam\_pkcs11.conf.example.gz".

##### **References:**

1. NIST SP 800-53 Revision 4 :: IA-5

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238233

Rule ID: SV-238233r880870\_rule

STIG ID: UBTU-20-010066

Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.4 Require MFA for Remote Network Access</b> Require MFA for remote network access.	●	●	●
v8	<b>6.5 Require MFA for Administrative Access</b> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	<b>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

#### 4.4.7 Configure pam\_lastlog module

`pam_lastlog` is a PAM module to display a line of information about the last login of the user. In addition, the module maintains the `/var/log/lastlog` file. Some applications may perform this function themselves. In such cases, this module is not necessary.

The module checks `LASTLOG_UID_MAX` option in `/etc/login.defs` and does not update or display last login records for users with UID higher than its value. If the option is not present or its value is invalid, no user ID limit is applied.

If the module is called in the auth or account phase, the accounts that were not used recently enough will be disallowed to log in. The check is not performed for the root account so the root is never locked out. It is also not performed for users with UID higher than the `LASTLOG_UID_MAX` value.

Options:

- `debug` - Print debug information.
- `silent` - Don't inform the user about any previous login, just update the `/var/log/lastlog` file. This option does not affect display of bad login attempts.
- `never` - If the `/var/log/lastlog` file does not contain any old entries for the user, indicate that the user has never previously logged in with a welcome message.
- `nodate` - Don't display the date of the last login.
- `noterm` - Don't display the terminal name on which the last login was attempted.
- `nohost` - Don't indicate from which host the last login was attempted.
- `nowtmp` - Don't update the `wtmp` entry.
- `noupdate` - Don't update any file.
- `showfailed` - Display number of failed login attempts and the date of the last failed attempt from `btmp`. The date is not displayed when `nodate` is specified.
- `inactive=<days>` - This option is specific for the auth or account phase. It specifies the number of days after the last login of the user when the user will be locked out by the module. The default value is 90.
- `unlimited` - If the `fsize` limit is set, this option can be used to override it, preventing failures on systems with large UID values that lead `lastlog` to become a huge sparse file.

#### *4.4.7.1 Ensure last successful account logon is displayed upon logon (Automated)*

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

- STIG

##### **Description:**

The operating system must display the date and time of the last successful account logon upon logon

##### **Rationale:**

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

##### **Audit:**

Verify users are provided with feedback on when account accesses last occurred. Check that "pam\_lastlog" is used and not silent with the following command:

```
# grep pam_lastlog /etc/pam.d/login  
session required pam_lastlog.so showfailed
```

If "pam\_lastlog" is missing from "/etc/pam.d/login" file, is not "required", or the "silent" option is present, this is a finding.

##### **Remediation:**

Configure the Ubuntu operating system to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/login".

Add the following line to the top of "/etc/pam.d/login":

```
session required pam_lastlog.so showfailed
```

##### **References:**

1. NIST SP 800-53 Revision 5 :: AC-9

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238373  
Rule ID: SV-238373r654294\_rule  
STIG ID: UBTU-20-010453  
Severity: CAT III

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

#### 4.4.8 Configure pam\_fai delay

`pam_fai delay` is a PAM module that can be used to set the delay on failure per-application. If no delay is given, `pam_fai delay` will use the value of `FAIL_DELAY` from `/etc/login.defs`.

Options:

- `debug` - Turns on debugging messages sent to syslog.
- `delay=N` - Set the delay on failure to `N` microseconds.

#### *4.4.8.1 Ensure login delay after failed logon attempt (Automated)*

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

- STIG

##### **Description:**

The operating system must enforce a delay of at least 4 seconds between logon prompts following a failed logon attempt.

##### **Rationale:**

Limiting the number of logon attempts over a certain time interval reduces the chances that an unauthorized user may gain access to an account.

##### **Audit:**

Verify the operating system enforces a delay of at least 4 seconds between logon prompts following a failed logon attempt with the following command:

```
# grep pam_faildelay /etc/pam.d/common-auth  
auth required pam_faildelay.so delay=4000000
```

If the line is not present or is commented out, this is a finding.

##### **Remediation:**

Configure the Ubuntu operating system to enforce a delay of at least 4 seconds between logon prompts following a failed logon attempt.

Edit the file "/etc/pam.d/common-auth" and set the parameter `pam_faildelay` to a value of 4000000 or greater:

```
auth required pam_faildelay.so delay=4000000
```

##### **References:**

1. NIST SP 800-53 Revision 5 :: CM-6 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238237  
Rule ID: SV-238237r653886\_rule  
STIG ID: UBTU-20-010075  
Severity: CAT III

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

#### *4.4.9 Ensure all current passwords uses the configured hashing algorithm (Manual)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Currently used passwords with out of date hashing algorithms may pose a security risk to the system.

##### **Rationale:**

In use passwords should always match the configured hashing algorithm for the system.

##### **Impact:**

If the administrator forces a password change, this could cause a large spike in CPU usage if a large number of users change their password during the same time.

##### **Audit:**

Run the following script to get a list of users that are not using the currently configured hashing algorithm:

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

{
    declare -A HASH_MAP=( ["y"]="yescrypt" ["1"]="md5" ["2"]="blowfish"
["5"]="SHA256" ["6"]="SHA512" ["g"]="gost-yescrypt" )

    CONFIGURED_HASH=$(sed -n "s/^\\s*ENCRYPT_METHOD\\s*\\(.*)\\s*$/\\1/p"
/etc/login.defs)

    for MY_USER in $(sed -n "s/^\\(.*):\\\\$.*\\1/p" /etc/shadow)
do
    CURRENT_HASH=$(sed -n "s/${MY_USER}:\\\$\\(.*)\\1/p" /etc/shadow)
    if [[ "${HASH_MAP["${CURRENT_HASH}"]^^}" != "${CONFIGURED_HASH^^}" ]];
then
        echo "The password for '${MY_USER}' is using
'${HASH_MAP["${CURRENT_HASH}"]}' instead of the configured
'${CONFIGURED_HASH}'."
    fi
done
}
```

Nothing should be returned

Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

## Remediation:

If the administrator wish to force an immediate change on all users as per the output of the audit, execute:

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

{
    UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
    awk -F: -v UID_MIN="${UID_MIN}" '$3 >= UID_MIN && $1 != "nfsnobody" { print $1 }' /etc/passwd | xargs -n 1 chage -d 0
}
```

**Note:** This could cause significant temporary CPU load on the system if a large number of users reset their passwords at the same time.

## References:

1. NIST SP 800-53 Rev. 5: IA-5, SC-28

## 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

## **4.5 User Accounts and Environment**

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

DRAFT

#### 4.5.1 Set Shadow Password Suite Parameters

While a majority of the password control parameters have been moved to PAM, some parameters are still available through the shadow password suite. Any changes made to `/etc/login.defs` will only be applied if the `usermod` command is used. If user IDs are added a different way, use the `chage` command to effect changes to individual user IDs.

DRAFT

#### *4.5.1.1 Ensure minimum days between password changes is configured (Automated)*

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

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

##### **Description:**

The `PASS_MIN_DAYS` parameter in `/etc/login.defs` allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that `PASS_MIN_DAYS` parameter be set to 1 or more days.

##### **Rationale:**

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

##### **Audit:**

Run the following command and verify `PASS_MIN_DAYS` conforms to site policy (no less than 1 day):

```
# grep PASS_MIN_DAYS /etc/login.defs
```

```
PASS_MIN_DAYS 1
```

Run the following command and Review list of users and `PAS_MIN_DAYS` to Verify that all users' `PAS_MIN_DAYS` conforms to site policy (no less than 1 day):

```
# awk -F : '(/^[:]+:[^!*]/ && $4 < 1){print $1 " " $4}' /etc/shadow
```

```
No <user>:<PASS_MIN_DAYS> should be returned
```

##### **Remediation:**

Set the `PASS_MIN_DAYS` parameter to 1 in `/etc/login.defs`:

```
PASS_MIN_DAYS 1
```

Modify user parameters for all users with a password set to match:

```
# chage --mindays 1 <user>
```

##### **Default Value:**

`PASS_MIN_DAYS 0`

## References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5
2. NIST SP 800-53 :: IA-5 (1) (d)

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023  
Vul ID: V-238202  
Rule ID: SV-238202r653781\_rule  
STIG ID: UBTU-20-010007  
Severity: CAT III

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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, T1078.002, T1078.003, T1078.004, T1110, T1110.001, T1110.002, T1110.003, T1110.004	TA0006	M1027

#### *4.5.1.2 Ensure password expiration is 365 days or less (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The `PASS_MAX_DAYS` parameter in `/etc/login.defs` allows an administrator to force passwords to expire once they reach a defined age.

##### **Rationale:**

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity. It is recommended that the `PASS_MAX_DAYS` parameter does not exceed 365 days and is greater than the value of `PASS_MIN_DAYS`.

##### **Audit:**

Run the following command and verify `PASS_MAX_DAYS` conforms to site policy, does not exceed 365 days, and is greater than `PASS_MIN_DAYS`:

```
# grep PASS_MAX_DAYS /etc/login.defs
PASS_MAX_DAYS 365
```

Run the following command and Review list of users and `PASS_MAX_DAYS` to verify that all users' `PASS_MAX_DAYS` conforms to site policy, does not exceed 365 days, and is no less than `PASS_MIN_DAYS`

```
# awk -F: '(/^[:^:]+:[^!*]/ && ($5>365 || $5~/([0-9]-1|\s*/)) {print $1 " " $5}' /etc/shadow
No <user>:<PASS_MAX_DAYS> should be returned
```

##### **Remediation:**

Set the `PASS_MAX_DAYS` parameter to conform to site policy in `/etc/login.defs` :

```
PASS_MAX_DAYS 365
```

Modify user parameters for all users with a password set to match:

```
# chage --maxdays 365 <user>
```

##### **Default Value:**

`PASS_MAX_DAYS 99999`

## References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>
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

The password expiration **must be greater than the minimum days between password changes** or users will be unable to change their password

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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, T1078.002, T1078.003, T1078.004, T1110, T1110.001, T1110.002, T1110.003, T1110.004	TA0006	M1027

#### *4.5.1.3 Ensure password expiration warning days is 7 or more (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The `PASS_WARN_AGE` parameter in `/etc/login.defs` allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the `PASS_WARN_AGE` parameter be set to 7 or more days.

##### **Rationale:**

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

##### **Audit:**

Run the following command and verify `PASS_WARN_AGE` conforms to site policy (No less than 7 days):

```
# grep PASS_WARN_AGE /etc/login.defs  
PASS_WARN_AGE 7
```

Verify all users with a password have their number of days of warning before password expires set to 7 or more:

Run the following command and Review list of users and `PASS_WARN_AGE` to verify that all users' `PASS_WARN_AGE` conforms to site policy (No less than 7 days):

```
# awk -F: '(/^[:]+:[^!*]/ && $6<7) {print $1 " " $6}' /etc/shadow  
No <user>:<PASS_WARN_AGE> should be returned
```

##### **Remediation:**

Set the `PASS_WARN_AGE` parameter to 7 in `/etc/login.defs`:

```
PASS_WARN_AGE 7
```

Modify user parameters for all users with a password set to match:

```
# chage --warndays 7 <user>
```

##### **Default Value:**

`PASS_WARN_AGE 7`

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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	TA0006	M1027

#### *4.5.1.4 Ensure inactive password lock is 30 days or less (Automated)*

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

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

##### **Description:**

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

##### **Rationale:**

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

##### **Audit:**

Run the following command and verify INACTIVE conforms to site policy (no more than 30 days):

```
# useradd -D | grep INACTIVE
INACTIVE=30
```

Verify all users with a password have Password inactive no more than 30 days after password expires:

Run the following command and Review list of users and INACTIVE to verify that all users' INACTIVE conforms to site policy (no more than 30 days):

```
# awk -F: '(/^[:^:]+:[^!*]/ && ($7~/(\s*|-1)/ || $7>30)) {print $1 " " $7}' /etc/shadow
No <user>:<INACTIVE> should be returned
```

## **Remediation:**

Run the following command to set the default password inactivity period to 30 days:

```
# useradd -D -f 30
```

Modify user parameters for all users with a password set to match:

```
# chage --inactive 30 <user>
```

## **Default Value:**

INACTIVE=-1

## **References:**

1. NIST SP 800-53 Revision 4 :: IA-4 e

## **Additional Information:**

A value of -1 would disable this setting

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238330  
Rule ID: SV-238330r654165\_rule  
STIG ID: UBTU-20-010409  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.		●	●

#### *4.5.1.5 Ensure all users last password change date is in the past (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

All users should have a password change date in the past.

##### **Rationale:**

If a user's recorded password change date is in the future then they could bypass any set password expiration.

##### **Audit:**

Run the following script to verify all users last password change was in the past:

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

{
    l_output2=""
    while read -r l_user; do
        l_change=$(chage --list $l_user | awk -F: '($1 ~
/^\\s*Last\\s+password\\s+change/ && $2 !~ /never/) {print $2}' | xargs)
        if [[ "$l_change" =~ ^([0-9]{4}-[0-9]{2}-[0-9]{2})$ ]]; then
            l_output2="$l_output2\n - User: \"$l_user\" last password change is
in the future \"$l_change\""
        fi
    done < <(awk -F: '($2 ~ /^[^*!xX\\n\\r][^\\n\\r]+/) {print $1}' /etc/shadow)
    if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass
        echo -e "\n- Audit Result:\n  ** PASS **\n - All user password changes
are in the past \n"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :$l_output2\n"
    fi
}
```

##### **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.

##### **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, T1078.002, T1078.003, T1078.004, T1110, T1110.001, T1110.002, T1110.003, T1110.004	TA0006	M1027

#### *4.5.1.6 Ensure ENCRYPT\_METHOD is SHA512 (Automated)*

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

- STIG

##### **Description:**

The operating system must encrypt all stored passwords with a FIPS 140-2 approved cryptographic hashing algorithm.

##### **Rationale:**

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

##### **Audit:**

Verify that the shadow password suite configuration is set to encrypt passwords with a FIPS 140-2 approved cryptographic hashing algorithm.

Check the hashing algorithm that is being used to hash passwords with the following command:

```
# cat /etc/login.defs | grep -i encrypt_method  
ENCRYPT_METHOD SHA512
```

If "ENCRYPT\_METHOD" does not equal SHA512 or greater, this is a finding.

##### **Remediation:**

Configure the Ubuntu operating system to encrypt all stored passwords.

Edit/modify the following line in the "/etc/login.defs" file and set "ENCRYPT\_METHOD" to SHA512:

```
ENCRYPT_METHOD SHA512
```

##### **References:**

1. NIST SP 800-53 Revision 5 :: IA-7

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238325

Rule ID: SV-238325r654150\_rule

STIG ID: UBTU-20-010404

Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.		●	●

#### *4.5.1.7 Ensure temporary accounts expiration time of 72 hours or less (Manual)*

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

- STIG

##### **Description:**

The operating system must provision temporary user accounts with an expiration time of 72 hours or less.

##### **Rationale:**

If temporary user accounts remain active when no longer needed or for an excessive period, these accounts may be used to gain unauthorized access. To mitigate this risk, automated termination of all temporary accounts must be set upon account creation.

Temporary accounts are established as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation.

If temporary accounts are used, the operating system must be configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours.

To address access requirements, many operating systems may be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

##### **Audit:**

Verify that the Ubuntu operating system expires temporary user accounts within 72 hours or less.

For every existing temporary account, run the following command to obtain its account expiration information:

```
# chage -l system_account_name | grep expires  
  
Password expires : Aug 07, 2019  
Account expires : Aug 07, 2019
```

Verify that each of these accounts has an expiration date set within 72 hours of account creation.

If any temporary account does not expire within 72 hours of that account's creation, this is a finding.

## **Remediation:**

If a temporary account must be created, configure the system to terminate the account after a 72-hour time period with the following command to set an expiration date on it. Substitute "system\_account\_name" with the account to be created.

```
# chage -E $(date -d "+3 days" +%F) system_account_name
```

## **References:**

1. NIST SP 800-53 :: AC-2 (2)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238196  
Rule ID: SV-238196r653763\_rule  
STIG ID: UBTU-20-010000  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>16.10 Ensure All Accounts Have An Expiration Date</b> Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

#### *4.5.1.8 Ensure root account is locked (Automated)*

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

- STIG

##### **Description:**

The operating system must prevent direct login into the root account.

##### **Rationale:**

To assure individual accountability and prevent unauthorized access, organizational users must be individually identified and authenticated.

A group authenticator is a generic account used by multiple individuals. Use of a group authenticator alone does not uniquely identify individual users. Examples of the group authenticator is the UNIX OS "root" user account, the Windows "Administrator" account, the "sa" account, or a "helpdesk" account.

For example, the UNIX and Windows operating systems offer a 'switch user' capability allowing users to authenticate with their individual credentials and, when needed, 'switch' to the administrator role. This method provides for unique individual authentication prior to using a group authenticator.

Users (and any processes acting on behalf of users) need to be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization, which outlines specific user actions that can be performed on the operating system without identification or authentication.

Requiring individuals to be authenticated with an individual authenticator prior to using a group authenticator allows for traceability of actions, as well as adding an additional level of protection of the actions that can be taken with group account knowledge.

##### **Audit:**

Verify the Ubuntu operating system prevents direct logins to the root account with the following command:

```
# passwd -S root  
root L 04/23/2020 0 99999 7 -1
```

If the output does not contain "L" in the second field to indicate the account is locked, this is a finding.

## **Remediation:**

Configure the Ubuntu operating system to prevent direct logins to the root account by performing the following operations:

```
# passwd -l root
```

## **References:**

1. NIST SP 800-53 Revision 4 :: IA-2 (5)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238329  
Rule ID: SV-238329r654162\_rule  
STIG ID: UBTU-20-010408  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

#### *4.5.1.9 Ensure password expiration is 60 days or less (Automated)*

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

- STIG

##### **Description:**

The `PASS_MAX_DAYS` parameter in `/etc/login.defs` allows an administrator to force passwords to expire once they reach a defined age.

##### **Rationale:**

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity. It is recommended that the `PASS_MAX_DAYS` parameter does not exceed 60 days and is greater than the value of `PASS_MIN_DAYS`.

##### **Audit:**

Run the following command and verify `PASS_MAX_DAYS` conforms to site policy, does not exceed 60 days, and is greater than `PASS_MIN_DAYS`:

```
# grep PASS_MAX_DAYS /etc/login.defs
PASS_MAX_DAYS 60
```

Run the following command and Review list of users and `PASS_MAX_DAYS` to verify that all users' `PASS_MAX_DAYS` conforms to site policy, does not exceed 365 days, and is no less than `PASS_MIN_DAYS`

```
# awk -F: '(/^[:]+:[^!*]/ && ($5>60 || $5~/([0-1]-1|\s*/)){print $1 " " $5}' /etc/shadow
No <user>:<PASS_MAX_DAYS> should be returned
```

##### **Remediation:**

Set the `PASS_MAX_DAYS` parameter to conform to site policy in `/etc/login.defs`:

```
PASS_MAX_DAYS 60
```

Modify user parameters for all users with a password set to match:

```
# chage --maxdays 60 <user>
```

##### **Default Value:**

`PASS_MAX_DAYS 99999`

## References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>
2. NIST SP 800-53 :: IA-5 (1) (d)

## Additional Information:

A value of -1 will disable password expiration

The password expiration must be greater than the minimum days between password changes or users will be unable to change their password

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238203  
Rule ID: SV-238203r653784\_rule  
STIG ID: UBTU-20-010008  
Severity: CAT III

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.		●	●

#### *4.5.1.10 Ensure emergency accounts are removed or disabled after 72 hours (Manual)*

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

- STIG

##### **Description:**

The operating system must automatically remove or disable emergency accounts after 72 hours.

##### **Rationale:**

Emergency accounts are different from infrequently used accounts (i.e., local logon accounts used by the organization's System Administrators when network or normal logon/access is not available). Infrequently used accounts are not subject to automatic termination dates. Emergency accounts are accounts created in response to crisis situations, usually for use by maintenance personnel. The automatic expiration or disabling time period may be extended as needed until the crisis is resolved; however, it must not be extended indefinitely. A permanent account should be established for privileged users who need long-term maintenance accounts.

##### **Audit:**

Verify the Ubuntu operating system expires emergency accounts within 72 hours or less.

For every emergency account, run the following command to obtain its account expiration information:

```
# chage -l account_name | grep expires  
  
Password expires : Aug 07, 2019  
Account expires : Aug 07, 2019
```

Verify each of these accounts has an expiration date set within 72 hours of account creation.

If any of these accounts do not expire within 72 hours of that account's creation, this is a finding.

## **Remediation:**

If an emergency account must be created, configure the system to terminate the account after a 72-hour time period with the following command to set an expiration date on it. Substitute "account\_name" with the account to be created.

```
# chage -E $(date -d "+3 days" +%F) account_name
```

## **References:**

1. NIST SP 800-53 Revision 4 :: AC-2 (2)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238331  
Rule ID: SV-238331r654168\_rule  
STIG ID: UBTU-20-010410  
Severity: CAT III

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

#### *4.5.1.11 Ensure immediate change to a permanent password (Manual)*

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

- STIG

##### **Description:**

The operating system must allow the use of a temporary password for system logons with an immediate change to a permanent password.

##### **Rationale:**

Without providing this capability, an account may be created without a password. Non-repudiation cannot be guaranteed once an account is created if a user is not forced to change the temporary password upon initial logon.

Temporary passwords are typically used to allow access when new accounts are created or passwords are changed. It is common practice for administrators to create temporary passwords for user accounts which allow the users to log on, yet force them to change the password once they have successfully authenticated.

##### **Audit:**

Verify a policy exists that ensures when a user account is created, it is created using a method that forces a user to change their password upon their next login.  
If a policy does not exist, this is a finding.

##### **Remediation:**

Create a policy that ensures when a user is created, it is created using a method that forces a user to change their password upon their next login.

Below are two examples of how to create a user account that requires the user to change their password upon their next login.

```
$ sudo chage -d 0 [UserName]
```

*OR*

```
$ sudo passwd -e [UserName]
```

##### **References:**

1. NIST SP 800-53 Revision 4 :: IA-5 (1) (f)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238361  
Rule ID: SV-238361r654258\_rule  
STIG ID: UBTU-20-010440  
Severity: CAT II

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

#### *4.5.2 Ensure system accounts are secured (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

There are a number of accounts provided with most distributions that are used to manage applications and are not intended to provide an interactive shell.

##### **Rationale:**

It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, most distributions set the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to the `nologin` shell. This prevents the account from potentially being used to run any commands.

## Audit:

Run the following script to verify all local system accounts:

- Do not have a valid login shell
- Are locked

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

{
    l_output="" l_output2=""
    l_valid_shells=$( awk -F\| '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^//{\s,/,\\|\|/,g;p}' | paste -s -d '|')
    a_users=(); a_ulock=() # initialize arrays
    while read -r l_user; do # Populate array with system accounts that have a
valid login shell
        a_users+=("$l_user")
    done <<(awk -v pat="$l_valid_shells" -F:
'($1!~/^(root|sync|shutdown|halt|^\+)| && $3<'"$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)"' && $(NF) ~ pat) { print $1 }' /etc/passwd)
    while read -r l_ulock; do # Populate array with system accounts that
aren't locked
        a_ulock+=("$l_ulock")
    done <<(awk -v pat="$l_valid_shells" -F: '($1!~/^(root|^+)| && $2!~/LK?/
&& $3<'"$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)"' && $(NF) ~ pat) {
print $1 }' /etc/passwd)
    if ! (( ${#a_users[@]} > 0 )); then
        l_output="$l_output\n - local system accounts login is disabled"
    else
        l_output2="$l_output2\n - There are \"$(printf '%s'
"${#a_users[@]}")\" system accounts with login enabled\n - List of
accounts:\n$(printf '%s\n' "${a_users[@]:0:$l_limit}")\n - end of list\n"
        fi
    if ! (( ${#a_ulock[@]} > 0 )); then
        l_output="$l_output\n - local system accounts are locked"
    else
        l_output2="$l_output2\n - There are \"$(printf '%s'
"${#a_ulock[@]}")\" system accounts that are not locked\n - List of
accounts:\n$(printf '%s\n' "${a_ulock[@]:0:$l_limit}")\n - end of list\n"
        fi
    unset a_users; unset a_ulock # Remove arrays
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n ** PASS **\n - * Correctly configured *
:n$l_output\n"
    else
        echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit
failure *\n:$l_output2"
        [ -n "$l_output" ] && echo -e "- * Correctly configured *
:n$l_output\n"
        fi
    }
}
```

## Note:

- The root, sync, shutdown, and halt users are exempted from requiring a non-login shell
- root is exempt from being locked

## Remediation:

Set the shell for any accounts returned by the audit to nologin:

```
# usermod -s $(which nologin) <user>
```

Lock any non root accounts returned by the audit:

```
# usermod -L <user>
```

The following script will:

- Set the shell for any accounts returned by the audit to nologin
- Lock any non root system accounts returned by the audit:

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

{
    l_output="" l_output2=""
    l_valid_shells="^($ awk -F'/' '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^//{s/,/\n/g;p}' | paste -s -d '|')$"
    a_users=(); a_ulock=() # initialize arrays
    while read -r l_user; do # change system accounts that have a valid login
shell to nolog shell
        echo -e "- System account \"\$l_user\" has a valid logon shell,
changing shell to \"$(which nologin)\""
        usermod -s "$(which nologin)" "\$l_user"
    done <<(awk -v pat="\$l_valid_shells" -F:
'($1!~/\(\root|sync|shutdown|halt\|^+\)/ && $3<"$(awk '/^\s*UID_MIN/{print \$2}' /etc/login.defs)"' && $(NF) ~ pat) { print \$1 }' /etc/passwd)
    while read -r l_ulock; do # Lock system accounts that aren't locked
        echo -e "- System account \"\$l_ulock\" is not locked, locking account"
        usermod -L "\$l_ulock"
    done <<(awk -v pat="\$l_valid_shells" -F: '($1!~/\(\root|^+\)/ && $2!~/LK?/
&& $3<"$(awk '/^\s*UID_MIN/{print \$2}' /etc/login.defs)"' && $(NF) ~ pat) {
print \$1 }' /etc/passwd)
}
```

## References:

1. NIST SP 800-53 Rev. 5: AC-2, AC-3, AC-5, 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
T1078, T1078.001, T1078.003	TA0005	M1026

#### *4.5.3 Ensure default group for the root account is GID 0 (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The usermod command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.

##### **Rationale:**

Using GID 0 for the `root` account helps prevent `root`-owned files from accidentally becoming accessible to non-privileged users.

##### **Audit:**

Run the following command and verify the result is 0 :

```
# grep "^\$root:" /etc/passwd | cut -f4 -d:  
0
```

##### **Remediation:**

Run the following command to set the `root` user default group to GID 0 :

```
# usermod -g 0 root
```

##### **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

#### *4.5.4 Ensure default user umask is 027 or more restrictive (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The user file-creation mode mask (`umask`) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (rwxrwxrwx), and for any newly created file it is 0666 (rw-rw-rw-). The `umask` modifies the default Linux permissions by restricting (masking) these permissions. The `umask` is not simply subtracted, but is processed bitwise. Bits set in the `umask` are cleared in the resulting file mode.

*umask can be set with either octal or Symbolic values*

- Octal (Numeric) Value - Represented by either three or four digits. ie `umask 0027` or `umask 027`. If a four digit `umask` is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- Symbolic Value - Represented by a comma separated list for User `u`, group `g`, and world/other `o`. The permissions listed are not masked by `umask`. ie a `umask` set by `umask u=rwx,g=rx,o=` is the Symbolic equivalent of the Octal `umask 027`. This `umask` would set a newly created directory with file mode `drwxr-x---` and a newly created file with file mode `rw-r-----`.

##### **Setting the default `umask`:**

- `pam_umask` module:
  - will set the `umask` according to the system default in `/etc/login.defs` and user settings, solving the problem of different `umask` settings with different shells, display managers, remote sessions etc.
  - `umask=<mask>` value in the `/etc/login.defs` file is interpreted as Octal
  - Setting `USERGROUPS_ENAB` to `yes` in `/etc/login.defs` (default):
    - will enable setting of the `umask` group bits to be the same as owner bits. (examples: 022 -> 002, 077 -> 007) for non-root users, if the uid is the same as gid, and username is the same as the primary group name
    - `userdel` will remove the user's group if it contains no more members, and `useradd` will create by default a group with the name of the user

- System Wide Shell Configuration File:
  - `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `.profile`, however this file is used to set an initial PATH or PS1 for all shell users of the system. *is only executed for interactive login shells, or shells executed with the --login parameter*
  - `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh`. It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
  - `/etc/bash.bashrc` - System wide version of `.bashrc`. `etc/bashrc` also invokes `/etc/profile.d/*.sh` if non-login shell, but redirects output to `/dev/null` if non-interactive. *Is only executed for interactive shells or if BASH\_ENV is set to /etc/bash.bashrc*

### *User Shell Configuration Files:*

- `~/.profile` - Is executed to configure your shell before the initial command prompt. *Is only read by login shells.*
- `~/.bashrc` - Is executed for interactive shells. *only read by a shell that's both interactive and non-login*

### **Rationale:**

Setting a very secure default value for `umask` ensures that users make a conscious choice about their file permissions. A default `umask` setting of `077` causes files and directories created by users to not be readable by any other user on the system. A `umask` of `027` would make files and directories readable by users in the same Unix group, while a `umask` of `022` would make files readable by every user on the system.

### **Impact:**

Setting `USERGROUPS_ENAB no` in `/etc/login.defs` may change the expected behavior of `useradd` and `userdel`.

Setting `USERGROUPS_ENAB yes` in `/etc/login.defs`

- `userdel` will remove the user's group if it contains no more members
- `useradd` will create by default a group with the name of the user.

## Audit:

Run the following to verify:

- A default user umask is set to enforce a newly created directories's permissions to be 750 (drwxr-x---), and a newly created file's permissions be 640 (rw-r-----), or more restrictive
- No less restrictive System Wide umask is set

Run the following script to verify that a default user umask is set enforcing a newly created directories's permissions to be 750 (drwxr-x---), and a newly created file's permissions be 640 (rw-r-----), or more restrictive:

```
#!/bin/bash

passing=""
grep -Eq '^\s*UMASK\s+(0[0-7][2-7]7|[0-7][2-7]7)\b' /etc/login.defs && grep
-Eqi '^\s*USERGROUPS_ENAB\s*"no"\b' /etc/login.defs && grep -Eq
'^\s*session\s+(optional|requisite|required)\s+pam_umask\.so\b'
/etc/pam.d/common-session && passing=true
grep -REiq '^\s*UMASK\s+\s*(0[0-7][2-7]7|[0-7][2-
7]7|u=(r?|w?|x?)(r?|w?|x?)(r?|w?|x?),g=(r?x?|x?r?),o=)\b' /etc/profile*
/etc/bash.bashrc* && passing=true
[ "$passing" = true ] && echo "Default user umask is set"
```

Verify output is: "Default user umask is set"

Run the following to verify that no less restrictive system wide umask is set:

```
# grep -RPi '^(|^#[^#]* )\s*umask\s+([0-7][0-7][01][0-7]\b|[0-7][0-7][0-
6]\b|[0-7][01][0-7]\b|[0-7][0-7][0-
6]\b|(u=[rwx]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+\b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(
,o=[rwx]{0,3})?\b)' /etc/login.defs /etc/profile* /etc/bash.bashrc*
```

No file should be returned

## **Remediation:**

Run the following command and remove or modify the `umask` of any returned files:

```
# grep -RPi '^(^|#[^#]* )\s*umask\s+([0-7][0-7][01][0-7]\b|[0-7][0-7][0-7][0-6]\b|[0-7][01][0-7]\b|[0-7][0-7][0-6]\b|(u=[rwx]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+\b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(,o=[rwx]{0,3}))?\b)' /etc/login.defs /etc/profile* /etc/bash.bashrc*
```

Follow **one** of the following methods to set the default user umask:

Edit `/etc/login.defs` and edit the `UMASK` and `USERGROUPS_ENAB` lines as follows:

```
UMASK 027
```

```
USERGROUPS_ENAB no
```

Edit `/etc/pam.d/common-session` and add or edit the following:

```
session optional          pam_umask.so
```

**OR**

Configure umask in one of the following files:

- A file in the `/etc/profile.d/` directory ending in `.sh`
- `/etc/profile`
- `/etc/bash.bashrc`

*Example: `/etc/profile.d/set_umask.sh`*

```
umask 027
```

**Note:** this method only applies to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked.

## **Default Value:**

UMASK 022

## **References:**

1. `pam_umask(8)`
2. 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	<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
T1565, T1565.001	TA0007	

#### 4.5.5 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/bash.bashrc - System wide version of bash.bashrc. etc/bash.bashrc also invokes /etc/profile.d/\*.sh if non-login shell, but redirects output to /dev/null if non-interactive. **Is only executed for interactive shells or if BASH\_ENV is set to /etc/bash.bashrc.**

##### Rationale:

Setting a timeout value reduces the window of opportunity for unauthorized user access to another user's shell session that has been left unattended. It also ends the inactive session and releases the resources associated with that session.

## Audit:

Run the following script to verify `TMOUT` is configured:

- as multiple lines, or a single line
- once, and only once
- in **one and only one** of the following locations:
  - A file in the `/etc/profile.d/` directory ending in `.sh`
  - `/etc/profile`
  - `/etc/bash.bashrc`
- Follows local site policy:
  - Not to exceed 900
  - Not equal to 0
- to be readonly
- to be exported

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

{
    l_output="" l_output2=""
    l_tmv_max="900"
    l_searchloc="/etc/bashrc /etc/bash.bashrc /etc/profile /etc/profile.d/*.sh"
    a_tmofile=()
    while read -r l_file; do
        [ -e "$l_file" ] && a_tmofile+=("$(readlink -f $l_file)")
    done < <(grep -PRils '^h*([^\n\r]+\h+)?TMOUT=\d+\b' $l_searchloc)
    if ! (( ${#a_tmofile[@]} > 0 )); then
        l_output2="$l_output2\n- TMOUT is not set"
    elif (( ${#a_tmofile[@]} > 1 )); then
        l_output2="$l_output2\n- TMOUT is set in multiple locations.\n - List of files
where TMOUT is set:\n$(printf '%s\n' "${a_tmofile[@]}")\n - end of list\n"
    else
        for l_file in ${a_tmofile[@]}; do
            if (( $(grep -Pci '^h*([^\n\r]+\h+)?TMOUT=\d+' "$l_file") > 1 )); then
                l_output2="$l_output2\n- TMOUT is set multiple times in \"$l_file\""
            else
                l_tmv=$(grep -Pi '^h*([^\n\r]+\h+)?TMOUT=\d+' "$l_file" | grep -Po '\d+')
                if (( "$l_tmv" > "$l_tmv_max" )); then
                    l_output2="$l_output\n- TMOUT is \"$l_tmv\" in \"$l_file\"\n - Should be
\"$l_tmv_max\" or less and not \"0\""
                else
                    l_output="$l_output\n- TMOUT is correctly set to \"$l_tmv\" in
\"$l_file\""
                    if grep -Piq '^h*([^\n\r]+\h+)?readonly\h+TMOUT\b' "$l_file"; then
                        l_output="$l_output\n- TMOUT is correctly set to \"readonly\" in
\"$l_file\""
                    else
                        l_output2="$l_output2\n- TMOUT is not set to \"readonly\""
                    fi
                    if grep -Piq '^(\h*|\h*[^\n\r]+\h*\h*;\h*)export\h+TMOUT\b' "$l_file"; then
                        l_output="$l_output\n- TMOUT is correctly set to \"export\" in
\"$l_file\""
                    else
                        l_output2="$l_output2\n- TMOUT is not set to \"export\""
                    fi
                fi
            fi
        done
        unset a_tmofile # Remove array
        if [ -z "$l_output2" ]; then
            echo -e "\n- Audit Result:\n ** PASS **\n - * Correctly configured *\n:$l_output\n"
        else
            echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit failure *\n:$l_output2"
            [ -n "$l_output" ] && echo -e "- * Correctly configured * :\n$l_output\n"
        fi
    }
}
```

## **Remediation:**

**Review** /etc/bash.bashrc, /etc/profile, and all files ending in \*.sh in the /etc/profile.d/ directory and remove or edit all TMOUT=\_n\_ entries to follow local site policy.

TMOUT should:

- Be configured once, as multiple lines, or a single line, in **one and only one** of the following locations:
  - A file in the /etc/profile.d/ directory ending in .sh
  - /etc/profile
  - /etc/bash.bashrc
- Not exceed 900
- Not be equal to 0

### *Multiple line example:*

```
TMOUT=900
readonly TMOUT
export TMOUT
```

### *Single line example:*

```
readonly TMOUT=900 ; export TMOUT
```

## **References:**

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

## **Additional Information:**

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files are also checked

Other methods of setting a timeout exist not covered here

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <p><u>4.3 Configure Automatic Session Locking on Enterprise Assets</u><br/> 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><br/> Automatically lock workstation sessions after a standard period of inactivity.</p>                                                                                                                                                                              | ●    | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques            | Tactics | Mitigations |
|----------------------------------------|---------|-------------|
| T1078, T1078.001, T1078.002, T1078.003 | TA0005  | M1026       |

## *4.5.6 Ensure default user umask is 077 or more restrictive (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

### **Rationale:**

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

### **Impact:**

Setting `USERGROUPS_ENAB no` in `/etc/login.defs` may change the expected behavior of `useradd` and `userdel`.

Setting `USERGROUPS_ENAB yes` in `/etc/login.defs`

- `userdel` will remove the user's group if it contains no more members
- `useradd` will create by default a group with the name of the user.

### **Audit:**

Verify the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Check for the value of the `UMASK` parameter in `/etc/login.defs` file with the following command:

**Note:** If the value of the `UMASK` parameter is set to `000` in `/etc/login.defs` file, the Severity is raised to a CAT I.

```
# grep -i umask /etc/login.defs
```

```
UMASK 077
```

If the value for the `UMASK` parameter is not `077`, or the `UMASK` parameter is missing or is commented out, refer to the remediation procedure below.

## **Remediation:**

Configure the operating system to define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Add or edit the line for the `UMASK` parameter in `/etc/login.defs` file to 077:

Add, uncomment or update the following line:

```
UMASK 077
```

## **Default Value:**

UMASK 022

## **References:**

1. `pam_umask(8)`

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238209

Rule ID: SV-238209r653802\_rule

STIG ID: UBTU-20-010016

Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

#### *4.5.7 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

#### **4.5.8 Ensure default user shell timeout is 600 seconds or less (Automated)**

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

- STIG

##### **Description:**

TMOUT is an environmental setting that determines the timeout of a shell in seconds.

- TMOUT=*n* - Sets the shell timeout to *n* seconds. A setting of TMOUT=0 disables timeout.
- readonly TMOUT- Sets the TMOUT environmental variable as readonly, preventing unwanted modification during run-time.
- export TMOUT - exports the TMOUT variable

##### **System Wide Shell Configuration Files:**

- /etc/profile - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the .bash\_profile, however this file is used to set an initial PATH or PS1 for all shell users of the system. *is only executed for interactive login shells, or shells executed with the --login parameter.*
- /etc/profile.d - /etc/profile will execute the scripts within /etc/profile.d/\*.sh. It is recommended to place your configuration in a shell script within /etc/profile.d to set your own system wide environmental variables.
- /etc/bash.bashrc - System wide version of bash.bashrc. etc/bash.bashrc also invokes /etc/profile.d/\*.sh if non-login shell, but redirects output to /dev/null if non-interactive. *Is only executed for interactive shells or if BASH\_ENV is set to /etc/bash.bashrc.*

##### **Rationale:**

Setting a timeout value reduces the window of opportunity for unauthorized user access to another user's shell session that has been left unattended. It also ends the inactive session and releases the resources associated with that session.

## Audit:

Run the following script to verify that TMOUT is configured to: include a timeout of no more than 600 seconds, to be readonly, to be exported, and is not being changed to a longer timeout.

```
#!/bin/bash

output1="" output2=""
[ -f /etc/bash.bashrc ] && BRC="/etc/bash.bashrc"
for f in "$BRC" /etc/profile /etc/profile.d/*.sh ; do
    grep -Pq '\bTMOUT=(600|[1-5][0-9]| [1-9][0-9]| [1-9])\b' "$f" && grep -Pq '\breadonly\h+TMOUT(\h+|\h*;|\h*$|=(600|[1-5][0-9]| [1-9][0-9]| [1-9]))\b' "$f" && grep -Pq '\bexport\h+([^\n\r]+\h+)?TMOUT\b' "$f" &&
    output1="$f"
done
output2=$(grep -Ps '\bTMOUT=(6[0-9][1-9]| [7-9][0-9]| [0-9]| [1-9]{3,}| 0+)\b' /etc/profile /etc/profile.d/*.sh $BRC)
if [ -n "$output1" ] && [ -z "$output2" ]; then
    echo -e "\nPASSED\nTMOUT is configured in: \"$output1\"\n"
else
    [ -z "$output1" ] && echo -e "\nFAILED\nTMOUT is not configured\n"
    [ -n "$output2" ] && echo -e "\nFAILED\nTMOUT is incorrectly configured
in: \"$output2\"\n"
fi
```

## Remediation:

**Review** /etc/bash.bashrc, /etc/profile, and all files ending in \*.sh in the /etc/profile.d/ directory and remove or edit all TMOUT=\_n\_ entries to follow local site policy. TMOUT should not exceed 900 or be equal to 0.

Configure TMOUT in one of the following files:

- A file in the /etc/profile.d/ directory ending in .sh
- /etc/profile
- /etc/bash.bashrc

**TMOUT configuration examples:**

- As multiple lines:
  -

```
TMOUT=600
readonly TMOUT
export TMOUT
```

- As a single line:

```
readonly TMOUT=600 ; export TMOUT
```

## **Additional Information:**

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files are also checked

Other methods of setting a timeout exist not covered here

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238207  
Rule ID: SV-238207r853404\_rule  
STIG ID: UBTU-20-010013  
Severity: CAT II

## **CIS Controls:**

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

## *4.6 Ensure /etc/ssl/certs only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must only allow the use of DoD PKI-established certificate authorities for verification of the establishment of protected sessions.

### **Rationale:**

Untrusted Certificate Authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DoD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DoD-approved CA, trust of this CA has not been established.

The DoD will only accept PKI-certificates obtained from a DoD-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of SSL/TLS certificates.

### **Audit:**

Verify the directory containing the root certificates for the Ubuntu operating system (/etc/ssl/certs) only contains certificate files for DoD PKI-established certificate authorities.

Determine if "/etc/ssl/certs" only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities with the following command:

```
# for f in $(ls /etc/ssl/certs); do openssl x509 -sha256 -in $f -noout -fingerprint | cut -d= -f2 | tr -d ':' | egrep -vw '(9676F287356C89A12683D65234098CB77C4F1C18F23C0E541DE0E196725B7EBE|B107B33F453E5510F68E513110C6F6944BACC263DF0137F821C1B3C2F8F863D2|559A5189452B13F8233F0022363C06F26E3C517C1D4B77445035959DF3244F74|1F4EDE9DC2A241F6521BF518424ACD49EBE84420E69DAF5BAC57AF1F8EE294A9)'; done
```

If any entry is found, this is a finding.

## **Remediation:**

Configure the Ubuntu operating system to only allow the use of DoD PKI-established certificate authorities for verification of the establishment of protected sessions.

Edit the "/etc/ca-certificates.conf" file, adding the character "!" to the beginning of all uncommented lines that do not start with the "!" character with the following command:

```
# sed -iE 's/^([#!#]+)!/\1/' /etc/ca-certificates.conf
```

Add at least one DoD certificate authority to the "/usr/local/share/ca-certificates" directory in the PEM format.

Update the "/etc/ssl/certs" directory with the following command:

```
# update-ca-certificates
```

## **References:**

1. NIST SP 800-53 Revision 5 :: SC-23 (5)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238364

Rule ID: SV-238364r654267\_rule

STIG ID: UBTU-20-010443

Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.1 Establish and Maintain a Secure Configuration Process</b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and 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>5.1 Establish Secure Configurations</b><br>Maintain documented, standard security configuration standards for all authorized operating systems and software.                                                                                                                                                                                                                                                       | ●    | ●    | ●    |

## 5 Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included in most distributions.

It is recommended that `rsyslog` be used for logging (with `logwatch` providing summarization) and `auditd` be used for auditing (with `aureport` providing summarization) to automatically monitor logs for intrusion attempts and other suspicious system behavior.

In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server via an encrypted connection. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized among systems and devices connected to the local network.

It is important that all logs described in this section be monitored on a regular basis and correlated to determine trends. A seemingly innocuous entry in one log could be more significant when compared to an entry in another log.

*Note on log file permissions: There really isn't a "one size fits all" solution to the permissions on log files. Many sites utilize group permissions so that administrators who are in a defined security group, such as "wheel" do not have to elevate privileges to root in order to read log files. Also, if a third party log aggregation tool is used, it may need to have group permissions to read the log files, which is preferable to having it run setuid to root. Therefore, there are two remediation and audit steps for log file permissions. One is for systems that do not have a secured group method implemented that only permits root to read the log files (`root:root 600`). The other is for sites that do have such a setup and are designated as `root:securegrp 640` where `securegrp` is the defined security group (in some cases `wheel`).*

## 5.1 Configure Logging

Logging services should be configured to prevent information leaks and to aggregate logs on a remote server so that they can be reviewed in the event of a system compromise. A centralized log server provides a single point of entry for further analysis, monitoring and filtering.

### Security principals for logging

- Ensure transport layer security is implemented between the client and the log server.
- Ensure that logs are rotated as per the environment requirements.
- Ensure all locally generated logs have the appropriate permissions.
- Ensure all security logs are sent to a remote log server.
- Ensure the required events are logged.

### What is covered

This section will cover the minimum best practices for the usage of **either rsyslog or journald**. The recommendations are written such that each is wholly independent of each other and **only one is implemented**.

- If your organization makes use of an enterprise wide logging system completely outside of `rsyslog` or `journald`, then the following recommendations does not directly apply. However, the principals of the recommendations should be followed regardless of what solution is implemented. If the enterprise solution incorporates either of these tools, careful consideration should be given to the following recommendations to determine exactly what applies.
- Should your organization make use of both `rsyslog` and `journald`, take care how the recommendations may or may not apply to you.

### What is not covered

- Enterprise logging systems not utilizing `rsyslog` or `journald`. As logging is very situational and dependant on the local environment, not everything can be covered here.
- Transport layer security should be applied to all remote logging functionality. Both `rsyslog` and `journald` supports secure transport and should be configured as such.
- The log server. There are a multitude of reasons for a centralized log server (and keeping a short period logging on the local system), but the log server is out of scope for these recommendations.

### 5.1.1 Configure journald

Included in the systemd suite is a journaling service called `systemd-journald.service` for the collection and storage of logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources such as:

- Classic RFC3164 BSD syslog via the `/dev/log` socket
- `STDOUT/STDERR` of programs via `StandardOutput=journal + StandardError=journal` in service files (both of which are default settings)
- Kernel log messages via the `/dev/kmsg` device node
- Audit records via the kernel's audit subsystem
- Structured log messages via `journald`'s native protocol

Any changes made to the `systemd-journald` configuration will require a re-start of `systemd-journald`

### **5.1.1.1 Ensure journald is configured to send logs to a remote log host**

DRAFT

### *5.1.1.1.1 Ensure systemd-journal-remote is installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

#### **Rationale:**

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

#### **Audit:**

Run the following command to verify `systemd-journal-remote` is installed.

Run the following command:

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
systemd-journal-remote  
  
systemd-journal-remote      install ok installed      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-12, SI-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●    | ●    | ●    |
| v7               | <b>6.3 Enable Detailed Logging</b><br>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       |

## 5.1.1.1.2 Ensure `systemd-journal-remote` is configured (Manual)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

### Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

### Audit:

Verify `systemd-journal-remote` is configured.

Run the following command:

```
# grep -P "^(?:(?!\s*#).)*URL=|^(?:(?!\s*#).)*ServerKeyFile=|^(?:(?!\s*#).)*ServerCertificateFile=|^(?:(?!\s*#).)*TrustedCertificateFile=" /etc/systemd/journal-upload.conf
```

Verify the output matches per your environments certificate locations and the URL of the log server. Example:

```
URL=192.168.50.42
ServerKeyFile=/etc/ssl/private/journal-upload.pem
ServerCertificateFile=/etc/ssl/certs/journal-upload.pem
TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

### Remediation:

Edit the `/etc/systemd/journal-upload.conf` file and ensure the following lines are set per your environment:

```
URL=192.168.50.42
ServerKeyFile=/etc/ssl/private/journal-upload.pem
ServerCertificateFile=/etc/ssl/certs/journal-upload.pem
TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Restart the service:

```
# systemctl restart systemd-journal-upload
```

### 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><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●    | ●    | ●    |
| v7               | <b>6.3 Enable Detailed Logging</b><br>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       |

### *5.1.1.1.3 Ensure systemd-journal-remote is enabled (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

#### **Rationale:**

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

#### **Audit:**

Verify `systemd-journal-remote` is enabled.

Run the following command:

```
# systemctl is-enabled systemd-journal-upload.service
```

Verify the output matches:

```
enabled
```

#### **Remediation:**

Run the following command to enable `systemd-journal-remote`:

```
# systemctl --now enable systemd-journal-upload.service
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, CM-7, SI-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●    | ●    | ●    |
| v7               | <b>6.3 Enable Detailed Logging</b><br>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       |

#### *5.1.1.1.4 Ensure journald is not configured to receive logs from a remote client (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Journald supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

##### **Note:**

- The same package, `systemd-journal-remote`, is used for both sending logs to remote hosts and receiving incoming logs.
- With regards to receiving logs, there are two services; `systemd-journal-remote.socket` and `systemd-journal-remote.service`.

##### **Rationale:**

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside its operational boundary.

##### **Audit:**

Run the following command to verify `systemd-journal-remote.socket` is not enabled:

```
# systemctl is-enabled systemd-journal-remote.socket
```

Verify the output matches:

```
disabled
```

##### **Remediation:**

Run the following command to disable `systemd-journal-remote.socket`:

```
# systemctl --now disable systemd-journal-remote.socket
```

##### **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, 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><br/>           Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p> |      | ●    | ●    |
| v8               | <p><b>8.2 Collect Audit Logs</b><br/>           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><br/>           Ensure that local logging has been enabled on all systems and networking devices.</p>                                                                                                                                      | ●    | ●    | ●    |
| v7               | <p><b>6.3 Enable Detailed Logging</b><br/>           Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>                                             |      | ●    | ●    |
| v7               | <p><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b><br/>           Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.006 | TA0040  | M1029       |

### *5.1.1.2 Ensure journald service is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Ensure that the `systemd-journald` service is enabled to allow capturing of logging events.

#### **Rationale:**

If the `systemd-journald` service is not enabled to start on boot, the system will not capture logging events.

#### **Audit:**

Run the following command to verify `systemd-journald` is enabled:

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

Verify the output matches:

```
static
```

#### **Remediation:**

By default the `systemd-journald` service does not have an `[Install]` section and thus cannot be enabled / disabled. It is meant to be referenced as `Requires` or `Wants` by other unit files. As such, if the status of `systemd-journald` is not static, investigate why.

#### **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               | <p><b>8.2 Collect Audit Logs</b><br/>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><br/>Ensure that local logging has been enabled on all systems and networking devices.</p>                                                                                          | ●    | ●    | ●    |
| v7               | <p><b>6.3 Enable Detailed Logging</b><br/>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p> |      | ●    | ●    |

## MITRE ATT&CK Mappings:

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

### *5.1.1.3 Ensure journald is configured to compress large log files (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The journald system includes the capability of compressing overly large files to avoid filling up the system with logs or making the logs unmanageably large.

#### **Rationale:**

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

#### **Audit:**

Run the following command to verify that large files will be compressed:

```
# grep -Psi '^h*Compress\h*=\\b' /etc/systemd/journald.conf  
/etc/systemd/journald.conf.d/*
```

Verify the output matches:

```
Compress=yes
```

#### **Remediation:**

Edit the `/etc/systemd/journald.conf` file or a file ending in `.conf` in `/etc/systemd/journald.conf.d/` and add the following line:

```
Compress=yes
```

Restart the service:

```
# systemctl restart systemd-journald
```

#### **References:**

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

## Additional Information:

The main configuration file `/etc/systemd/journald.conf` is read before any of the custom `*.conf` files. If there are custom configs present, they override the main configuration parameters.

It is possible to change the default threshold of 512 bytes per object before compression is used.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●    | ●    | ●    |
| v7               | <b>6.3 Enable Detailed Logging</b><br>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><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                                                                      |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.002            | TA0040  | M1053       |

#### *5.1.1.4 Ensure journald is configured to write logfiles to persistent disk (Automated)*

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

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Data from journald may be stored in volatile memory or persisted locally on the server. Logs in memory will be lost upon a system reboot. By persisting logs to local disk on the server they are protected from loss due to a reboot.

##### **Rationale:**

Writing log data to disk will provide the ability to forensically reconstruct events which may have impacted the operations or security of a system even after a system crash or reboot.

##### **Audit:**

Run the following command to verify that logs are persisted to disk:

```
# grep -Psi '^h*Storage\h*=\\h*persistent\b' /etc/systemd/journald.conf  
/etc/systemd/journald.conf.d/*
```

Verify the output matches:

```
Storage=persistent
```

##### **Remediation:**

Edit the `/etc/systemd/journald.conf` file or a file ending in `.conf` in `/etc/systemd/journald.conf.d/` and add the following line:

```
Storage=persistent
```

Restart the service:

```
# systemctl restart systemd-journald
```

##### **References:**

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

##### **Additional Information:**

The main configuration file `/etc/systemd/journald.conf` is read before any of the custom `*.conf` files. If there are custom configs present, they override the main configuration parameters.

**Note:** a bug in systemd versions prior to v243 caused an error at the unmounting of /var/log (and thus, /var) if Storage=persistent is set in /etc/systemd/journald.conf.

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●    | ●    | ●    |
| v7               | <b>6.3 Enable Detailed Logging</b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |      | ●    | ●    |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.006 | TA0005  | M1022       |

### *5.1.1.5 Ensure journald is not configured to send logs to rsyslog (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Data from `journald` should be kept in the confines of the service and not forwarded on to other services.

#### **Rationale:**

If `journald` is the method for capturing logs, all logs of the system should be handled by `journald` and not forwarded to other logging mechanisms.

#### **Audit:**

If `journald` is the method for capturing logs

Run the following command to verify that logs are not forwarded to `rsyslog`:

```
# grep -Psi '^h*ForwardToSyslog|h*=\\b` /etc/systemd/journald.conf  
/etc/systemd/journald.conf.d/*
```

Verify that there is no output.

#### **Remediation:**

Edit the `/etc/systemd/journald.conf` file and files in `/etc/systemd/journald.conf.d/` and ensure that `ForwardToSyslog=yes` is removed.

Restart the service:

```
# systemctl restart systemd-journald
```

#### **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><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         | ●    | ●    | ●    |
| v8               | <b>8.9 Centralize Audit Logs</b><br>Centralize, to the extent possible, audit log collection and retention across enterprise assets.                                                                            |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●    | ●    | ●    |
| v7               | <b>6.3 Enable Detailed Logging</b><br>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>6.5 Central Log Management</b><br>Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.                                                              |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.006 | TA0040  | M1029       |

### *5.1.1.6 Ensure journald log rotation is configured per site policy (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Journald includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file `/etc/systemd/journald.conf` is the configuration file used to specify how logs generated by Journald should be rotated.

#### **Rationale:**

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

#### **Audit:**

Review `/etc/systemd/journald.conf`, and files in `/etc/systemd/journald.conf.d/`, and verify logs are rotated according to site policy. The specific parameters for log rotation are:

```
SystemMaxUse=
SystemKeepFree=
RuntimeMaxUse=
RuntimeKeepFree=
MaxFileSec=
```

#### **Remediation:**

Review `/etc/systemd/journald.conf` and verify logs are rotated according to site policy. The settings should be carefully understood as there are specific edge cases and prioritisation of parameters.

The specific parameters for log rotation are:

```
SystemMaxUse=
SystemKeepFree=
RuntimeMaxUse=
RuntimeKeepFree=
MaxFileSec=
```

#### **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><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●    | ●    | ●    |
| v7               | <b>6.3 Enable Detailed Logging</b><br>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       |

## *5.1.1.7 Ensure journald default file permissions configured (Manual)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Journald will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

### **Rationale:**

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

### **Audit:**

First see if there is an override file `/etc/tmpfiles.d/systemd.conf`. If so, this file will override all default settings as defined in `/usr/lib/tmpfiles.d/systemd.conf` and should be inspected.

If there is no override file, inspect the default `/usr/lib/tmpfiles.d/systemd.conf` against the site specific requirements.

Ensure that file permissions are 0640.

Should a site policy dictate less restrictive permissions, ensure to follow said policy.

**NOTE:** More restrictive permissions such as 0600 is implicitly sufficient.

### **Remediation:**

If the default configuration is not appropriate for the site specific requirements, copy `/usr/lib/tmpfiles.d/systemd.conf` to `/etc/tmpfiles.d/systemd.conf` and modify as required. Requirements is either 0640 or site policy if that is less restrictive.

### **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><br/> Configure data access control lists based on a 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>8.2 Collect Audit Logs</b><br/> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.</p>                                                                                 | ●    | ●    | ●    |
| v7               | <p><b>5.1 Establish Secure Configurations</b><br/> Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>                                                                                         | ●    | ●    | ●    |
| v7               | <p><b>6.2 Activate audit logging</b><br/> Ensure that local logging has been enabled on all systems and networking devices.</p>                                                                                                                                  | ●    | ●    | ●    |
| v7               | <p><b>6.3 Enable Detailed Logging</b><br/> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>                                         |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  |             |

## 5.1.2 Configure rsyslog

The `rsyslog` software package may be used instead of the default `journald` logging mechanism.

**Note:** This section only applies if `rsyslog` is the chosen method for client side logging. Do not apply this section if `journald` is used.

DRAFT

### *5.1.2.1 Ensure rsyslog is installed (Automated)*

#### **Profile Applicability:**

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

#### **Description:**

The `rsyslog` software is a recommended replacement to the original `syslogd` daemon which provide improvements over `syslogd`, such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

#### **Rationale:**

The security enhancements of `rsyslog` such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

#### **Audit:**

Verify either `rsyslog` or `syslog-ng` is installed. Use the following command to provide the needed information:

```
# dpkg -s rsyslog
```

#### **Remediation:**

Install `rsyslog`:

```
# apt install rsyslog
```

#### **References:**

1. NIST SP 800-53 Revision 4 :: SC-24

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238353

Rule ID: SV-238353r654234\_rule

STIG ID: UBTU-20-010432

Severity: CAT II

## **CIS Controls:**

| <b>Controls Version</b> | <b>Control</b>                                                                                                                                                                                                  | <b>IG 1</b> | <b>IG 2</b> | <b>IG 3</b> |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-------------|
| v8                      | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●           | ●           | ●           |
| v7                      | <b>6.3 Enable Detailed Logging</b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |             | ●           | ●           |

### *5.1.2.2 Ensure rsyslog service is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Once the `rsyslog` package is installed, ensure that the service is enabled.

#### **Rationale:**

If the `rsyslog` service is not enabled to start on boot, the system will not capture logging events.

#### **Audit:**

Run the following command to verify `rsyslog` is enabled:

```
# systemctl is-enabled rsyslog
```

Verify the output matches:

```
enabled
```

#### **Remediation:**

Run the following command to enable `rsyslog`:

```
# systemctl --now enable rsyslog
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <p><b>8.2 Collect Audit Logs</b><br/>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><br/>Ensure that local logging has been enabled on all systems and networking devices.</p>                                                                                          | ●    | ●    | ●    |
| v7               | <p><b>6.3 Enable Detailed Logging</b><br/>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p> |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.001 | TA0005  | M1028       |

### *5.1.2.3 Ensure journald is configured to send logs to rsyslog (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Data from `journald` may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of `journald` logs, however, use of the RSyslog service provides a consistent means of log collection and export.

#### **Rationale:**

**IF** RSyslog is the preferred method for capturing logs, all logs of the system should be sent to it for further processing.

#### **Audit:**

**IF** RSyslog is the preferred method for capturing logs

Review `/etc/systemd/journald.conf` and verify that logs are forwarded to `rsyslog`.

```
# grep ^\s*ForwardToSyslog /etc/systemd/journald.conf
```

Verify the output matches:

```
ForwardToSyslog=yes
```

#### **Remediation:**

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
ForwardToSyslog=yes
```

Restart the service:

```
# systemctl restart rsyslog
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-9

## **Additional Information:**

As noted in the `journald` man pages, `journald` logs may be exported to `rsyslog` either through the process mentioned here, or through a facility like `systemd-journald.service`. There are trade-offs involved in each implementation, where `ForwardToSyslog` will immediately capture all events (and forward to an external log server, if properly configured), but may not capture all boot-up activities. Mechanisms such as `systemd-journald.service`, on the other hand, will record bootup events, but may delay sending the information to `rsyslog`, leading to the potential for log manipulation prior to export. Be aware of the limitations of all tools employed to secure a system.

The main configuration file `/etc/systemd/journald.conf` is read before any of the custom `*.conf` files. If there are custom configurations present, they override the main configuration parameters

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         | ●    | ●    | ●    |
| v8               | <b>8.9 Centralize Audit Logs</b><br>Centralize, to the extent possible, audit log collection and retention across enterprise assets.                                                                            |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●    | ●    | ●    |
| v7               | <b>6.3 Enable Detailed Logging</b><br>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>6.5 Central Log Management</b><br>Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.                                                              |      | ●    | ●    |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1070, T1070.002, T1562, T1562.006 | TA0040         | M1029              |

DRAFT

## *5.1.2.4 Ensure rsyslog default file permissions are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

RSyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

### **Rationale:**

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

### **Impact:**

The systems global `umask` could override, but only making the file permissions stricter, what is configured in RSyslog with the `FileCreateMode` directive. RSyslog also has its own `$umask` directive that can alter the intended file creation mode. In addition, consideration should be given to how `FileCreateMode` is used.

Thus it is critical to ensure that the intended file creation mode is not overridden with less restrictive settings in `/etc/rsyslog.conf`, `/etc/rsyslog.d/*conf` files and that `FileCreateMode` is set before any file is created.

### **Audit:**

Run the following command:

```
# grep ^\$FileCreateMode /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Verify the output matches:

```
$FileCreateMode 0640
```

Should a site policy dictate less restrictive permissions, ensure to follow said policy.

**NOTE:** More restrictive permissions such as 0600 is implicitly sufficient.

## Remediation:

Edit either `/etc/rsyslog.conf` or a dedicated `.conf` file in `/etc/rsyslog.d/` and set `$FileCreateMode` to 0640 or more restrictive:

```
$FileCreateMode 0640
```

Restart the service:

```
# systemctl restart rsyslog
```

## References:

1. See the `rsyslog.conf(5)` man page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, AC-6, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                                                                 | ●    | ●    | ●    |
| v7               | <b>5.1 Establish Secure Configurations</b><br>Maintain documented, standard security configuration standards for all authorized operating systems and software.                                                                                         | ●    | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                  | ●    | ●    | ●    |
| v7               | <b>6.3 Enable Detailed Logging</b><br>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, T1083, T1083.000 | TA0007         | M1028              |

DRAFT

### 5.1.2.5 Ensure logging is configured (Manual)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files specifies rules for logging and which files are to be used to log certain classes of messages.

#### Rationale:

A great deal of important security-related information is sent via `rsyslog` (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

#### Audit:

Review the contents of `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files to ensure appropriate logging is set. In addition, run the following command and verify that the log files are logging information as expected:

```
# ls -l /var/log/
```

#### Remediation:

Edit the following lines in the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files as appropriate for your environment.

**NOTE:** The below configuration is shown for example purposes only. Due care should be given to how the organization wish to store log data.

|                                      |                                      |
|--------------------------------------|--------------------------------------|
| <code>*.emerg</code>                 | <code>:omusrmsg:*</code>             |
| <code>auth,authpriv.*</code>         | <code>/var/log/secure</code>         |
| <code>mail.*</code>                  | <code>-/var/log/mail</code>          |
| <code>mail.info</code>               | <code>-/var/log/mail.info</code>     |
| <code>mail.warning</code>            | <code>-/var/log/mail.warn</code>     |
| <code>mail.err</code>                | <code>-/var/log/mail.err</code>      |
| <code>cron.*</code>                  | <code>-/var/log/cron</code>          |
| <code>*.=warning;*.=err</code>       | <code>-/var/log/warn</code>          |
| <code>*.crit</code>                  | <code>-/var/log/warn</code>          |
| <code>*.*;mail.none;news.none</code> | <code>-/var/log/messages</code>      |
| <code>local0,local1.*</code>         | <code>-/var/log/localmessages</code> |
| <code>local2,local3.*</code>         | <code>-/var/log/localmessages</code> |
| <code>local4,local5.*</code>         | <code>-/var/log/localmessages</code> |
| <code>local6,local7.*</code>         | <code>-/var/log/localmessages</code> |

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

## References:

1. See the rsyslog.conf(5) man page for more information.
2. 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><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●    | ●    | ●    |
| v7               | <b>6.3 Enable Detailed Logging</b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. | ●    | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1070, T1070.002            | TA0005  | M1028       |

## 5.1.2.6 Ensure rsyslog is configured to send logs to a remote log host (Manual)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

RSyslog supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

### Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

### Audit:

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that logs are sent to a central host (where `loghost.example.com` is the name of your central log host):

#### Old format

```
# grep "^\.*[^I][^I]*@" /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include @@<FQDN or IP of remote loghost>, for example

```
.* @loghost.example.com
```

#### New format

```
# grep -E '^s*([^\#]+\s+)?action\(([^\#]+\s+)?\bttarget="?[^"]+"?\b' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include target=<FQDN or IP of remote loghost>, for example:

```
.* action(type="omfwd" target="loghost.example.com" port="514" protocol="tcp"
```

## Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and add the following line (where `loghost.example.com` is the name of your central log host). The `target` directive may either be a fully qualified domain name or an IP address.

```
*.* action(type="omfwd" target="192.168.2.100" port="514" protocol="tcp"  
        action.resumeRetryCount="100"  
        queue.type="LinkedList" queue.size="1000")
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

## References:

1. See the `rsyslog.conf(5)` man page for more information.
2. NIST SP 800-53 Rev. 5: AU-6

## Additional Information:

In addition, see the [RSyslog documentation](#) for implementation details of TLS.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●    | ●    | ●    |
| v7               | <b>6.3 Enable Detailed Logging</b><br>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       |

### *5.1.2.7 Ensure remote access methods are monitored (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must monitor remote access methods

#### **Rationale:**

Remote access services, such as those providing remote access to network devices and information systems, which lack automated monitoring capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Automated monitoring of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

#### **Audit:**

Verify that the Ubuntu operating system monitors all remote access methods. Check that remote access methods are being logged by running the following command:

```
# grep -E -r '^(auth,authpriv\.\.*|daemon\.\*)' /etc/rsyslog.*  
/etc/rsyslog.d/50-default.conf:auth,authpriv.* /var/log/auth.log  
/etc/rsyslog.d/50-default.conf:daemon.notice /var/log/messages
```

If "auth.", "authpriv.", or "daemon.\*" are not configured to be logged in at least one of the config files, this is a finding.

## **Remediation:**

Configure the Ubuntu operating system to monitor all remote access methods by adding the following lines to the "/etc/rsyslog.d/50-default.conf" file:

```
auth.*,authpriv.* /var/log/secure  
daemon.notice /var/log/messages
```

For the changes to take effect, restart the "rsyslog" service with the following command:

```
# systemctl restart rsyslog.service
```

## **References:**

1. NIST SP 800-53 Revision 5 :: AC-17 (1)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238324  
Rule ID: SV-238324r654147\_rule  
STIG ID: UBTU-20-010403  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.1 Establish and Maintain a Secure Configuration Process</b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and 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>5.1 Establish Secure Configurations</b><br>Maintain documented, standard security configuration standards for all authorized operating systems and software.                                                                                                                                                                                                                                                       | ●    | ●    | ●    |

### *5.1.2.8 Ensure rsyslog is not configured to receive logs from a remote client (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

RSyslog supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

#### **Rationale:**

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside its operational boundary.

#### **Audit:**

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that the system is not configured to accept incoming logs.

#### **Old format**

```
# grep '$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf  
# grep '$InputTCPServerRun' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

No output expected.

#### **New format**

```
# grep -P -- '^h*module\(load="imtcp")' /etc/rsyslog.conf  
/etc/rsyslog.d/*.conf  
# grep -P -- '^h*input\(type="imtcp" port="514")' /etc/rsyslog.conf  
/etc/rsyslog.d/*.conf
```

No output expected.

## **Remediation:**

Should there be any active log server configuration found in the auditing section, modify those file and remove the specific lines highlighted by the audit. Ensure none of the following entries are present in any of `/etc/rsyslog.conf` or `/etc/rsyslog.d/*.conf`.

### **Old format**

```
$ModLoad imtcp  
$InputTCPServerRun
```

### **New format**

```
module(load="imtcp")  
input(type="imtcp" port="514")
```

Restart the service:

```
# systemctl restart rsyslog
```

### **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               | <p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b><br/>           Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p> |      | ●    | ●    |
| v8               | <p><b>8.2 Collect Audit Logs</b><br/>           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><br/>           Ensure that local logging has been enabled on all systems and networking devices.</p>                                                                                                                                      | ●    | ●    | ●    |
| v7               | <p><b>6.3 Enable Detailed Logging</b><br/>           Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>                                             |      | ●    | ●    |
| v7               | <p><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b><br/>           Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.006 | TA0005  | M1028       |

### **5.1.3 Configure logfile access**

Logfiles may contain sensitive information. Access needs to be configured to allow only the appropriate users and/or groups access to them

DRAFT

### *5.1.3.1 Ensure /var/log is owned by root (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must configure the /var/log directory to be owned by root.

#### **Rationale:**

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

#### **Audit:**

Verify the Ubuntu operating system configures the "/var/log" directory to be owned by root with the following command:

```
# stat -c "%n %U" /var/log  
/var/log root
```

If the "/var/log" directory is not owned by root, this is a finding.

#### **Remediation:**

Configure the Ubuntu operating system to have root own the "/var/log" directory by running the following command:

```
# chown root /var/log
```

#### **References:**

1. NIST SP 800-53 Revision 5 :: SI-11 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238339

Rule ID: SV-238339r654192\_rule

STIG ID: UBTU-20-010418

Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

### *5.1.3.2 Ensure /var/log is group-owned by syslog (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must configure the /var/log directory to be group-owned by syslog.

#### **Rationale:**

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

#### **Audit:**

Verify that the Ubuntu operating system configures the "/var/log" directory to be group-owned by syslog with the following command:

```
# stat -c "%n %G" /var/log  
/var/log syslog
```

If the "/var/log" directory is not group-owned by syslog, this is a finding.

#### **Remediation:**

Configure the Ubuntu operating system to have syslog group-own the "/var/log" directory by running the following command:

```
# chgrp syslog /var/log
```

#### **References:**

1. NIST SP 800-53 Revision 5 :: SI-11 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238338

Rule ID: SV-238338r654189\_rule

STIG ID: UBTU-20-010417

Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

### *5.1.3.3 Ensure /var/log is mode 0755 or more restrictive (Automated)*

#### **Profile Applicability:**

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

#### **Description:**

Log files stored in `/var/log/` contain logged information from many services on the system, or on log hosts others as well.

#### **Rationale:**

It is important to ensure that `/var/log` has the correct permissions to ensure that sensitive data is archived and protected.

#### **Audit:**

Run the following command to verify that `/var/log/` is mode 0755 or more restrictive:

```
# stat -c '%n %a' /var/log/  
/var/log 755
```

#### **Remediation:**

Run the following command to remove additional assess on `/var/log/`:

```
chmod go-w /var/log/
```

#### **References:**

1. NIST SP 800-53 Revision 5 :: SI-11 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238340  
Rule ID: SV-238340r880879\_rule  
STIG ID: UBTU-20-010419  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

### *5.1.3.4 Ensure all logfiles have appropriate access configured (Automated)*

#### **Profile Applicability:**

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

#### **Description:**

Log files stored in `/var/log/` contain logged information from many services on the system and potentially from other logged hosts as well.

#### **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\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%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="${l_fname##$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
}
```

DRAFT

**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 is captured in the event that the remediation causes issues.

DRAFT

```

#!/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-rx,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 access configured.

## References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2
2. NIST SP 800-53 :: SI-11

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238337  
Rule ID: SV-238337r880876\_rule  
STIG ID: UBTU-20-010416  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>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  | M1028       |

### *5.1.3.5 Ensure /var/log/syslog is owned by syslog (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must configure /var/log/syslog file to be owned by syslog.

#### **Rationale:**

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

#### **Audit:**

Verify that the Ubuntu operating system configures the "/var/log/syslog" file to be owned by syslog with the following command:

```
# stat -c "%n %U" /var/log/syslog  
/var/log/syslog syslog
```

If the "/var/log/syslog" file is not owned by syslog, this is a finding.

#### **Remediation:**

Configure the Ubuntu operating system to have syslog own the "/var/log/syslog" file by running the following command:

```
# chown syslog /var/log/syslog
```

#### **References:**

1. NIST SP 800-53 Revision 5 :: SI-11 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238342

Rule ID: SV-238342r654201\_rule

STIG ID: UBTU-20-010421

Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

### *5.1.3.6 Ensure /var/log/syslog is group-owned by adm (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must configure the /var/log/syslog file to be group-owned by adm.

#### **Rationale:**

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

#### **Audit:**

Verify that the Ubuntu operating system configures the "/var/log/syslog" file to be group-owned by adm with the following command:

```
# stat -c "%n %G" /var/log/syslog
/var/log/syslog adm
```

If the "/var/log/syslog" file is not group-owned by adm, this is a finding.

#### **Remediation:**

Configure the Ubuntu operating system to have adm group-own the "/var/log/syslog" file by running the following command:

```
# chgrp adm /var/log/syslog
```

#### **References:**

1. NIST SP 800-53 Revision 5 :: SI-11 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238341  
Rule ID: SV-238341r654198\_rule  
STIG ID: UBTU-20-010420  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

### *5.1.3.7 Ensure /var/log/syslog is 0640 or more restrictive (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must configure /var/log/syslog file with mode 0640 or less permissive.

#### **Rationale:**

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

#### **Audit:**

Verify that the Ubuntu operating system configures the "/var/log/syslog" file with mode 0640 or less permissive by running the following command:

```
# stat -c "%n %a" /var/log/syslog
/var/log/syslog 640
```

If a value of "640" or less permissive is not returned, this is a finding.

#### **Remediation:**

Configure the Ubuntu operating system to have permissions of 0640 for the "/var/log/syslog" file by running the following command:

```
# chmod 0640 /var/log/syslog
```

#### **References:**

1. NIST SP 800-53 Revision 5 :: SI-11 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238343

Rule ID: SV-238343r654204\_rule

STIG ID: UBTU-20-010422

Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

## 5.2 Configure System Accounting (auditd)

The Linux Auditing System operates on a set of rules that collects certain types of system activity to facilitate incident investigation, detect unauthorized access or modification of data. By default events will be logged to `/var/log/audit/audit.log`, which can be configured in `/etc/audit/auditd.conf`.

The following types of audit rules can be specified:

- Control rules: Configuration of the auditing system.
- File system rules: Allow the auditing of access to a particular file or a directory. Also known as file watches.
- System call rules: Allow logging of system calls that any specified program makes.

Audit rules can be set:

- On the command line using the `auditctl` utility. These rules are not persistent across reboots.
- In `/etc/audit/audit.rules`. These rules have to be merged and loaded before they are active.

### Notes:

- For 64 bit systems that have `arch` as a rule parameter, you will need two rules: one for 64 bit and one for 32 bit systems calls. For 32 bit systems, only one rule is needed.
- If the auditing system is configured to be locked (`-e 2`), a system reboot will be required in order to load any changes.
- Key names are optional on the rules and will not be used as a compliance auditing. The usage of key names is highly recommended as it facilitates organisation and searching, as such, all remediation steps will have key names supplied.
- It is best practice to store the rules, in number prepended files, in `/etc/audit/rules.d/`. Rules must end in a `.rules` suffix. This then requires the use of `augenrules` to merge all the rules into `/etc/audit/audit.rules` based on their their alphabetical (lexical) sort order. All benchmark recommendations follow this best practice for remediation, specifically using the prefix of 50 which is centre weighed if all rule sets make use of the number prepending naming convention.
- Your system may have been customized to change the default `UID_MIN`. All samples output uses 1000, but this value will not be used in compliance auditing. To confirm the `UID_MIN` for your system, run the following command: `awk '/^s*UID_MIN/{print $2}' /etc/login.defs`

## Normalization

The Audit system normalizes some entries, so when you look at the sample output keep in mind that:

- With regards to users whose login UID is not set, the values `-1` / `unset` / `4294967295` are equivalent and normalized to `-1`.
- When comparing field types and both sides of the comparison is valid fields types, such as `euid!=uid`, then the auditing system may normalize such that the output is `uid!=euid`.
- Some parts of the rule may be rearranged whilst others are dependant on previous syntax. For example, the following two statements are the same:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F auid==1 -F  
key=user_emulation
```

and

```
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k  
user_emulation
```

## Capacity planning

The recommendations in this section implement auditing policies that not only produces large quantities of logged data, but may also negatively impact system performance. Capacity planning is critical in order not to adversely impact production environments.

- Disk space. If a significantly large set of events are captured, additional on system or off system storage may need to be allocated. If the logs are not sent to a remote log server, ensure that log rotation is implemented else the disk will fill up and the system will halt. Even when logs are sent to a log server, ensure sufficient disk space to allow caching of logs in the case of temporary network outages.
- Disk IO. It is not just the amount of data collected that should be considered, but the rate at which logs are generated.
- CPU overhead. System call rules might incur considerable CPU overhead. Test the systems open/close syscalls per second with and without the rules to gauge the impact of the rules.

### **5.2.1 Ensure auditing is enabled**

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

DRAFT

### 5.2.1.1 Ensure auditd is installed (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

auditd is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk

#### Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

#### Audit:

Run the following command and verify auditd and audispd-plugins are installed:

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'  
auditd  
  
auditd install ok installed installed
```

#### Remediation:

Run the following command to Install auditd

```
# apt install auditd
```

#### 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               | <b>8.5 Collect Detailed Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.001            | TA0005  | M1028       |

DRAFT

### *5.2.1.2 Ensure auditd service is enabled and active (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Turn on the `auditd` daemon to record system events.

#### **Rationale:**

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

#### **Audit:**

Run the following command to verify `auditd` is enabled:

```
# systemctl is-enabled auditd  
enabled
```

Verify result is "enabled".

Run the following command to verify `auditd` is active:

```
# systemctl is-active auditd  
active
```

Verify result is active

#### **Remediation:**

Run the following command to enable and start `auditd`:

```
# systemctl --now enable auditd
```

#### **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><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●    | ●    | ●    |
| v7               | <b>6.3 Enable Detailed Logging</b><br>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       |

### *5.2.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Configure `grub2` so that processes that are capable of being audited can be audited even if they start up prior to `auditd` startup.

#### **Rationale:**

Audit events need to be captured on processes that start up prior to `auditd`, so that potential malicious activity cannot go undetected.

#### **Audit:**

Run the following command:

```
# find -L /boot -type f -name 'grub.cfg' -exec grep -Ph -- '^h*linux\b' {} + | grep -v 'audit=1'
```

Nothing should be returned.

#### **Remediation:**

Edit `/etc/default/grub` and add `audit=1` to `GRUB_CMDLINE_LINUX`:

Example:

```
GRUB_CMDLINE_LINUX="audit=1"
```

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

```
# update-grub
```

#### **Additional Information:**

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

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                    | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <p><b>8.2 Collect Audit Logs</b><br/>           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><br/>           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       |

### *5.2.1.4 Ensure audit\_backlog\_limit is sufficient (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

In the kernel-level audit subsystem, a socket buffer queue is used to hold audit events. Whenever a new audit event is received, it is logged and prepared to be added to this queue.

The kernel boot parameter `audit_backlog_limit=N`, with `N` representing the amount of messages, will ensure that a queue cannot grow beyond a certain size. If an audit event is logged which would grow the queue beyond this limit, then a failure occurs and is handled according to the system configuration

#### **Rationale:**

If an audit event is logged which would grow the queue beyond the `audit_backlog_limit`, then a failure occurs, auditd records will be lost, and potential malicious activity could go undetected.

#### **Audit:**

Run the following command and verify the `audit_backlog_limit=` parameter is set:

```
# find -L /boot -type f -name 'grub.cfg' -exec grep -Ph -- '^\\h*linux\\b' {} + | 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><br/>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><br/>Ensure that local logging has been enabled on all systems and networking devices.</p>                                                                                          | ●    | ●    | ●    |
| v7               | <p><b>6.3 Enable Detailed Logging</b><br/>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, M1047 |

### **5.2.2 Configure Data Retention**

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, auditd will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, check your site policy for audit storage requirements.

DRAFT

### *5.2.2.1 Ensure audit log storage size is configured (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.

#### **Rationale:**

It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

#### **Audit:**

Run the following command and ensure output is in compliance with site policy:

```
# grep -Po -- '^h*max_log_file\h*=\h*\d+\b' /etc/audit/auditd.conf  
max_log_file = <MB>
```

#### **Remediation:**

Set the following parameter in `/etc/audit/auditd.conf` in accordance with site policy:

```
max_log_file = <MB>
```

#### **Default Value:**

```
max_log_file = 8
```

#### **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               | <b>8.3 Ensure Adequate Audit Log Storage</b><br>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><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0040  | M1047       |

## 5.2.2.2 Ensure audit logs are not automatically deleted (Automated)

### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

### Description:

The `max_log_file_action` setting determines how to handle the audit log file reaching the max file size. A value of `keep_logs` will rotate the logs but never delete old logs.

### Rationale:

In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

### Audit:

Run the following command and verify output matches:

```
# grep max_log_file_action /etc/audit/auditd.conf
max_log_file_action = keep_logs
```

### Remediation:

Set the following parameter in `/etc/audit/auditd.conf`:

```
max_log_file_action = keep_logs
```

### 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><br>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><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |      | ●    | ●    |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  | M1047       |

DRAFT

### *5.2.2.3 Ensure system is disabled when audit logs are full (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The `auditd` daemon can be configured to halt the system when the audit logs are full.

The `admin_space_left_action` parameter tells the system what action to take when the system has detected that it is low on disk space. Valid values are `ignore`, `syslog`, `suspend`, `single`, and `halt`.

- `ignore`, the audit daemon does nothing
- `Syslog`, the audit daemon will issue a warning to syslog
- `Suspend`, the audit daemon will stop writing records to the disk
- `single`, the audit daemon will put the computer system in single user mode
- `halt`, the audit daemon will shutdown the system

#### **Rationale:**

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

#### **Impact:**

If the `admin_space_left_action` parameter is set to `halt` the audit daemon will shutdown the system when the disk partition containing the audit logs becomes full.

#### **Audit:**

Run the following commands and verify output matches:

```
# grep space_left_action /etc/audit/auditd.conf
space_left_action = email
# grep action_mail_acct /etc/audit/auditd.conf
action_mail_acct = root
```

Run the following command and verify the output is either `halt` **or** `single`:

```
# grep -E 'admin_space_left_action\s*=\s*(halt|single)'
/etc/audit/auditd.conf
admin_space_left_action = <halt|single>
```

## **Remediation:**

Set the following parameters in /etc/audit/auditd.conf:

```
space_left_action = email  
action_mail_acct = root
```

set admin\_space\_left\_action to either halt or single in /etc/audit/auditd.conf.

*Example:*

```
admin_space_left_action = halt
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-8, AU-12, SI-5

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                  | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>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><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |      | ●    | ●    |

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

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  | M1028       |

#### *5.2.2.4 Ensure crontab script running to offload audit events of standalone systems (Manual)*

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

- STIG

##### **Description:**

The operating system must have a crontab script running weekly to offload audit events of standalone systems.

##### **Rationale:**

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

##### **Audit:**

**Note:** If this is an interconnected system, this is Not Applicable.

Verify there is a script that offloads audit data and that script runs weekly.

Check if there is a script in the "/etc/cron.weekly" directory that offloads audit data:

```
# ls /etc/cron.weekly  
audit-offload
```

Check if the script inside the file does offloading of audit logs to external media.

If the script file does not exist or does not offload audit logs, this is a finding.

##### **Remediation:**

Create a script that offloads audit logs to external media and runs weekly.

The script must be located in the "/etc/cron.weekly" directory.

##### **References:**

1. NIST SP 800-53 Revision 5 :: AU-4 (1)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238321  
Rule ID: SV-238321r654138\_rule  
STIG ID: UBTU-20-010300  
Severity: CAT III

## **CIS Controls:**

| <b>Controls Version</b> | <b>Control</b>                                                                                                                                                                                                                                                                                                                                                                                            | <b>IG 1</b> | <b>IG 2</b> | <b>IG 3</b> |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-------------|
| v8                      | <b>8.1 Establish and Maintain an Audit Log Management Process</b><br>Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ●           | ●           | ●           |
| v7                      | <b>6.4 Ensure adequate storage for logs</b><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                                                                                                                                                                                                                                                                | ●           | ●           | ●           |
| v7                      | <b>6.5 Central Log Management</b><br>Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.                                                                                                                                                                                                                                                        | ●           | ●           | ●           |

## *5.2.2.5 Ensure shut down by default upon audit failure (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must shut down by default upon audit failure (unless availability is an overriding concern).

### **Rationale:**

It is critical that when the operating system is at risk of failing to process audit logs as required, it takes action to mitigate the failure. Audit processing failures include: software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Responses to audit failure depend upon the nature of the failure mode.

When availability is an overriding concern, other approved actions in response to an audit failure are as follows:

1. If the failure was caused by the lack of audit record storage capacity, the operating system must continue generating audit records if possible (automatically restarting the audit service if necessary), overwriting the oldest audit records in a first-in-first-out manner.
2. If audit records are sent to a centralized collection server and communication with this server is lost or the server fails, the operating system must queue audit records locally until communication is restored or until the audit records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local audit data with the collection server.

### **Audit:**

Verify the Ubuntu operating system takes the appropriate action when the audit storage volume is full with the following command:

```
# grep '^disk_full_action' /etc/audit/auditd.conf  
disk_full_action = HALT
```

If the value of the "disk\_full\_action" option is not "SYSLOG", "SINGLE", or "HALT", or the line is commented out, this is a finding.

## **Remediation:**

Configure the Ubuntu operating system to shut down by default upon audit failure (unless availability is an overriding concern).

Add or update the following line (depending on configuration, "disk\_full\_action" can be set to "SYSLOG", "HALT" or "SINGLE") in "/etc/audit/auditd.conf" file:

```
disk_full_action = HALT
```

Restart the "auditd" service so the changes take effect:

```
# systemctl restart auditd.service
```

## **References:**

1. NIST SP 800-53 Revision 5 :: AU-5 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238244

Rule ID: SV-238244r653907\_rule

STIG ID: UBTU-20-010118

Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. | ●    | ●    | ●    |
| v7               | <b>6.4 Ensure adequate storage for logs</b><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                              |      | ●    | ●    |

## *5.2.2.6 Ensure security personnel are notified when storage volume reaches 75 percent utilization (Manual)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must immediately notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity.

### **Rationale:**

If security personnel are not notified immediately when storage volume reaches 75% utilization, they are unable to plan for audit record storage capacity expansion.

### **Audit:**

Verify the Ubuntu operating system notifies the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity with the following command:

```
# grep ^space_left_action /etc/audit/auditd.conf  
  
space_left_action email  
# grep ^space_left /etc/audit/auditd.conf  
  
space_left 250000
```

If the "space\_left" parameter is missing, set to blanks, or set to a value less than 25% of the space free in the allocated audit record storage, this is a finding.

If the "space\_left\_action" parameter is missing or set to blanks, this is a finding.

If the "space\_left\_action" is set to "syslog", the system logs the event but does not generate a notification, and this is a finding.

If the "space\_left\_action" is set to "exec", the system executes a designated script. If this script informs the SA of the event, this is not a finding.

If the "space\_left\_action" is set to "email", check the value of the "action\_mail\_acct" parameter with the following command:

```
# grep ^action_mail_acct /etc/audit/auditd.conf  
  
action_mail_acct root@localhost
```

The "action\_mail\_acct" parameter, if missing, defaults to "root". If the "action\_mail\_acct" parameter is not set to the email address of the SA(s) and/or ISSO, this is a finding.

**Note:** If the email address of the System Administrator is on a remote system, a mail package must be available.

## **Remediation:**

Edit "/etc/audit/auditd.conf" and set the "space\_left\_action" parameter to "exec" or "email".

If the "space\_left\_action" parameter is set to "email", set the "action\_mail\_acct" parameter to an email address for the SA and ISSO.

If the "space\_left\_action" parameter is set to "exec", ensure the command being executed notifies the SA and ISSO.

Edit "/etc/audit/auditd.conf" and set the "space\_left" parameter to be at least 25% of the repository maximum audit record storage capacity.

## **References:**

1. NIST SP 800-53 Revision 5 :: AU-5 (1)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238307

Rule ID: SV-238307r654096\_rule

STIG ID: UBTU-20-010217

Severity: CAT III

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                  | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.3 Ensure Adequate Audit Log Storage</b><br>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><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |      | ●    | ●    |

## *5.2.2.7 Ensure sufficient storage capacity to store at least one week worth of audit records (Manual)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must allocate audit record storage capacity to store at least one weeks' worth of audit records, when audit records are not immediately sent to a central audit record storage facility.

### **Rationale:**

In order to ensure operating systems have a sufficient storage capacity in which to write the audit logs, operating systems need to be able to allocate audit record storage capacity.

### **Audit:**

Verify the Ubuntu operating system allocates audit record storage capacity to store at least one week's worth of audit records when audit records are not immediately sent to a central audit record storage facility.

Determine which partition the audit records are being written to with the following command:

```
# grep ^log_file /etc/audit/auditd.conf  
log_file = /var/log/audit/audit.log
```

Check the size of the partition that audit records are written to (with the example being "/var/log/audit") with the following command:

```
# df -h /var/log/audit/  
/dev/sda2 24G 10.4G 13.6G 43% /var/log/audit
```

If the audit records are not written to a partition made specifically for audit records (""/var/log/audit" is a separate partition), determine the amount of space being used by other files in the partition with the following command:

```
# du -sh [audit_partition]  
1.8G /var/log/audit
```

**Note:** The partition size needed to capture a week's worth of audit records is based on the activity level of the system and the total storage capacity available. In normal circumstances, 10.0 GB of storage space for audit records will be sufficient.

If the audit record partition is not allocated for sufficient storage capacity, this is a finding.

## **Remediation:**

Allocate enough storage capacity for at least one week's worth of audit records when audit records are not immediately sent to a central audit record storage facility.

If audit records are stored on a partition made specifically for audit records, use the "parted" program to resize the partition with sufficient space to contain one week's worth of audit records.

If audit records are not stored on a partition made specifically for audit records, a new partition with sufficient amount of space will need to be created.

Set the auditd server to point to the mount point where the audit records must be located:

```
# sed -i -E 's@^(log_file\s*=\\s*) .*@\1 <log mountpoint>/audit.log@' /etc/audit/auditd.conf
```

where is the aforementioned mount point.

## **References:**

1. NIST SP 800-53 Revision 5 :: AU-4

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238305

Rule ID: SV-238305r654090\_rule

STIG ID: UBTU-20-010215

Severity: CAT III

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                  | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.3 Ensure Adequate Audit Log Storage</b><br>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><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |      | ●    | ●    |

## *5.2.2.8 Ensure audit event multiplexor is configured to off-load audit logs onto a different system or storage media from the system being audited (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system audit event multiplexor must be configured to off-load audit logs onto a different system or storage media from the system being audited.

### **Rationale:**

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

### **Audit:**

Verify the audit event multiplexor is configured to offload audit records to a different system or storage media from the system being audited.

Check that audisp-remote plugin is installed:

```
# dpkg -s audispd-plugins
```

If status is "not installed", this is a finding.

Check that the records are being offloaded to a remote server with the following command:

```
# grep -i active /etc/audisp/plugins.d/au-remote.conf  
active = yes
```

If "active" is not set to "yes", or the line is commented out, this is a finding.

Check that audisp-remote plugin is configured to send audit logs to a different system:

```
# grep -i ^remote_server /etc/audisp/audisp-remote.conf  
remote_server = 192.168.122.126
```

If the "remote\_server" parameter is not set, is set with a local address, or is set with an invalid address, this is a finding.

## **Remediation:**

Configure the audit event multiplexor to offload audit records to a different system or storage media from the system being audited.

Install the audisp-remote plugin:

```
# apt-get install audispd-plugins -y
```

Set the audisp-remote plugin as active by editing the "/etc/audisp/plugins.d/au-remote.conf" file:

```
# sed -i -E 's/active\s*=\\s*no/active = yes/' /etc/audisp/plugins.d/au-remote.conf
```

Set the address of the remote machine by editing the "/etc/audisp/audisp-remote.conf" file:

```
# sed -i -E 's/(remote_server\s*=).*/\1 <remote addr>/' /etc/audisp/audisp-remote.conf
```

where must be substituted by the address of the remote server receiving the audit log.  
Make the audit service reload its configuration files:

```
# systemctl restart auditd.service
```

## **References:**

1. NIST SP 800-53 Revision 5 :: AU-4 (1)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238306  
Rule ID: SV-238306r654093\_rule  
STIG ID: UBTU-20-010216  
Severity: CAT III

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.1 Establish and Maintain a Secure Configuration Process</b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and 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>5.1 Establish Secure Configurations</b><br>Maintain documented, standard security configuration standards for all authorized operating systems and software.                                                                                                                                                                                                                                                       | ●    | ●    | ●    |

### 5.2.3 Configure auditd rules

The Audit system operates on a set of rules that define what is to be captured in the log files.

The following types of Audit rules can be specified:

- Control rules: Allow the Audit system's behavior and some of its configuration to be modified.
- File system rules: Allow the auditing of access to a particular file or a directory. (Also known as file watches)
- System call rules: Allow logging of system calls that any specified program makes.

Audit rules can be set:

- on the command line using the `auditctl` utility. Note that these rules are not persistent across reboots.
- in a file ending in `.rules` in the `/etc/audit/audit.d/` directory.

### *5.2.3.1 Ensure changes to system administration scope (`sudoers`) is collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Monitor scope changes for system administrators. If the system has been properly configured to force system administrators to log in as themselves first and then use the `sudo` command to execute privileged commands, it is possible to monitor changes in scope. The file `/etc/sudoers`, or files in `/etc/sudoers.d`, will be written to when the file(s) or related attributes have changed. The audit records will be tagged with the identifier "scope".

#### **Rationale:**

Changes in the `/etc/sudoers` and `/etc/sudoers.d` files can indicate that an unauthorized change has been made to the scope of system administrator activity.

#### **Audit:**

##### **On disk configuration**

##### **Run the following command to check the on disk rules:**

```
# awk '/^ *-w/ \
&&!/etc/sudoers/ \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

##### **Running configuration**

##### **Run the following command to check loaded rules:**

```
# auditctl -l | awk '/^ *-w/ \
&&!/etc/sudoers/ \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor scope changes for system administrators.

Example:

```
# printf "
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
" >> /etc/audit/rules.d/50-scope.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **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><br>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><br>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:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1562, T1562.006                   | TA0004         | M1047              |

DRAFT

### *5.2.3.2 Ensure actions as another user are always logged (Automated)*

#### **Profile Applicability:**

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

#### **Description:**

`sudo` provides users with temporary elevated privileges to perform operations, either as the superuser or another user.

#### **Rationale:**

Creating an audit log of users with temporary elevated privileges and the operation(s) they performed is essential to reporting. Administrators will want to correlate the events written to the audit trail with the records written to `sudo`'s logfile to verify if unauthorized commands have been executed.

## Audit:

### 64 Bit systems

#### ***On disk configuration***

Run the following command to check the on disk rules:

```
# awk '/^ *-a *always,exit/ \
&& / -F *arch=b[2346]{2}/ \
&& / -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[2346]{2}/ \
&& / -F *auid!=unset||| -F *auid!=-1||| -F *auid!=4294967295/) \
&& / -C *euid!=uid||| -C *uid!=euid/) \
&& / -S *execve/ \
&& / key= *[!-~]* *$/||| -k *[!-~]* *$/) '
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F auid!=-1 -F
key=user_emulation
-a always,exit -F arch=b32 -S execve -C uid!=euid -F auid!=-1 -F
key=user_emulation
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor elevated privileges.

### **64 Bit systems**

Example:

```
# printf "
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
-a always,exit -F arch=b32 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
" >> /etc/audit/rules.d/50-user_emulation.rules
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **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.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238304  
Rule ID: SV-238304r654087\_rule  
STIG ID: UBTU-20-010211  
Severity: CAT II

Satisfies: SRG-OS-000326-GPOS-00126, SRG-OS-000327-GPOS-00127

### **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>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>4.9 Log and Alert on Unsuccessful Administrative Account Login</b><br>Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.                                                                                                                 |      | ●    | ●    |

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

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0004  | M1047       |

### *5.2.3.3 Ensure events that modify the sudo log file are collected (Automated)*

#### **Profile Applicability:**

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

#### **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:

### On disk configuration

Run the following command to check the on disk rules:

```
# {
  SUDO_LOG_FILE_ESCAPED=$(grep -r logfile /etc/sudoers* | sed -e
's/.*logfile=//;s/,? .*/' -e 's///g' -e 's|/|\\||g')
  [ -n "${SUDO_LOG_FILE_ESCAPED}" ] && awk "/^ *-w/ \
&&/"${SUDO_LOG_FILE_ESCAPED}"/ \
&&/+-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/) " /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'SUDO_LOG_FILE_ESCAPED' is unset.\n"
}
```

Verify output of matches:

```
-w /var/log/sudo.log -p wa -k sudo_log_file
```

### Running configuration

Run the following command to check loaded rules:

```
# {
  SUDO_LOG_FILE_ESCAPED=$(grep -r logfile /etc/sudoers* | sed -e
's/.*logfile=//;s/,? .*/' -e 's///g' -e 's|/|\\||g')
  [ -n "${SUDO_LOG_FILE_ESCAPED}" ] && auditctl -l | awk "/^ *-w/ \
&&/"${SUDO_LOG_FILE_ESCAPED}"/ \
&&/+-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/) " \
|| printf "ERROR: Variable 'SUDO_LOG_FILE_ESCAPED' is unset.\n"
}
```

Verify output matches:

```
-w /var/log/sudo.log -p wa -k sudo_log_file
```

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the sudo log file.

Example:

```
# {
SUDO_LOG_FILE=$(grep -r logfile /etc/sudoers* | sed -e 's/.*/logfile=//;s/,??
.*//' -e 's/"//g')
[ -n "${SUDO_LOG_FILE}" ] && printf "
-w ${SUDO_LOG_FILE} -p wa -k sudo_log_file
" >> /etc/audit/rules.d/50-sudo.rules || printf "ERROR: Variable
'SUDO_LOG_FILE_ESCAPED' is unset.\n"
}
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **References:**

1. NIST SP 800-53 Rev. 5: AU-3
2. NIST SP 800-53 Revision 4 :: AU-12 c
3. NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

## **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.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238309  
Rule ID: SV-238309r654102\_rule  
STIG ID: UBTU-20-010244  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <p><b>8.5 Collect Detailed Audit Logs</b><br/> 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><br/> 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       |

#### *5.2.3.4 Ensure events that modify date and time information are collected (Automated)*

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

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the;

- `adjtimex` - tune kernel clock
- `settimeofday` - set time using `timeval` and `timezone` structures
- `stime` - using seconds since 1/1/1970
- `clock_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:

### 64 Bit systems

#### ***On disk configuration***

Run the following command to check the on disk rules:

```
# {
awk '/^ *-a *always,exit/ \
&& -F *arch=b[2346]{2}/ \
&& -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[2346]{2}/ \
&& -S/ \
&&(/adjtimex/ \
||/settimeofday/ \
||/clock_settime/ ) \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' 

auditctl -l | awk '/^ *-w/ \
&&/etc/localtime/ \
&& +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' 
}
```

#### Verify the output includes:

```
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -F
key=time-change
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime -F
key=time-change
-w /etc/localtime -p wa -k time-change
```

## **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with b64. In addition, also audit for the stime system call rule. For example:

```
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime,stime -k  
time-change
```

### **Remediation:**

#### **Create audit rules**

Edit or create a file in the /etc/audit/rules.d/ directory, ending in .rules extension, with the relevant rules to monitor events that modify date and time information.

## **64 Bit systems**

### **Example:**

```
# printf "  
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -k time-  
change  
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime -k time-  
change  
-w /etc/localtime -p wa -k time-change  
" >> /etc/audit/rules.d/50-time-change.rules
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with b64. In addition, add stime to the system call audit. Example:

```
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime,stime -k  
time-change
```

### **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><br>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><br>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  | M1047       |

### *5.2.3.5 Ensure events that modify the system's network environment are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Record changes to network environment files or system calls. The below parameters monitors the following system calls, and write an audit event on system call exit:

- `sethostname` - set the systems host name
- `setdomainname` - set the systems domain name

The files being monitored are:

- `/etc/issue` and `/etc/issue.net` - messages displayed pre-login
- `/etc/hosts` - file containing host names and associated IP addresses
- `/etc/networks` - symbolic names for networks
- `/etc/network/` - directory containing network interface scripts and configurations files

#### **Rationale:**

Monitoring `sethostname` and `setdomainname` will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The `/etc/hosts` file is monitored for changes that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring `/etc/issue` and `/etc/issue.net` is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring `/etc/network` is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records should have a relevant tag associated with them.

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following commands to check the on disk rules:

```
# awk '/^ *-a *always,exit/ \
&& / -F *arch=b(32|64)/ \
&& / -S/ \
&& (/sethostname/ \
||/setdomainname/) \
&& (/ key= *[!~]* *$/||/ -k *[!~]* *$/) ' /etc/audit/rules.d/*.rules

# awk '/^ *-w/ \
&& (/etc/issue/ \
||/etc/issue.net/ \
||/etc/hosts/ \
||/etc/network/) \
&& / +p *wa/ \
&& (/ key= *[!~]* *$/||/ -k *[!~]* *$/) ' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S sethostname,setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname,setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/networks -p wa -k system-locale
-w /etc/network/ -p wa -k system-locale
```

#### *Running configuration*

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-a *always,exit/ \
&& / -F *arch=b(32|64)/ \
&& / -S/ \
&& (/sethostname/ \
||/setdomainname/) \
&& (/ key= *[!~]* *$/||/ -k *[!~]* *$/) '

# auditctl -l | awk '/^ *-w/ \
&& (/etc/issue/ \
||/etc/issue.net/ \
||/etc/hosts/ \
||/etc/network/) \
&& / +p *wa/ \
&& (/ key= *[!~]* *$/||/ -k *[!~]* *$/) '
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S sethostname,setdomainname -F key=system-locale
-a always,exit -F arch=b32 -S sethostname,setdomainname -F key=system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/networks -p wa -k system-locale
-w /etc/network/ -p wa -k system-locale
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the system's network environment.

#### **64 Bit systems**

Example:

```
# printf "
-a always,exit -F arch=b64 -S sethostname,setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname,setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/networks -p wa -k system-locale
-w /etc/network/ -p wa -k system-locale
" >> /etc/audit/rules.d/50-system_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
```

#### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **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><br>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><br>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       |

### *5.2.3.6 Ensure use of privileged commands are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Monitor privileged programs, those that have the `setuid` and/or `setgid` bit set on execution, to determine if unprivileged users are running these commands.

#### **Rationale:**

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

#### **Impact:**

Both the audit and remediation section of this recommendation will traverse all mounted file systems that is not mounted with either `noexec` or `nosuid` mount options. If there are large file systems without these mount options, **such traversal will be significantly detrimental to the performance of the system.**

Before running either the audit or remediation section, inspect the output of the following command to determine exactly which file systems will be traversed:

```
# findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid"
```

To exclude a particular file system due to adverse performance impacts, update the audit and remediation sections by adding a sufficiently unique string to the `grep` statement. The above command can be used to test the modified exclusions.

## Audit:

### On disk configuration

Run the following command to check on disk rules:

```
# for PARTITION in $(findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid" | awk '{print $1}'); do
    for PRIVILEGED in $(find "${PARTITION}" -xdev -perm /6000 -type f); do
        grep -qr "${PRIVILEGED}" /etc/audit/rules.d && printf "OK:
'${PRIVILEGED}' found in auditing rules.\n" || printf "Warning:
'${PRIVILEGED}' not found in on disk configuration.\n"
    done
done
```

Verify that all output is OK.

### Running configuration

Run the following command to check loaded rules:

```
# {
    RUNNING=$(auditctl -l)
    [ -n "${RUNNING}" ] && for PARTITION in $(findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid" | awk '{print $1}'); do
        for PRIVILEGED in $(find "${PARTITION}" -xdev -perm /6000 -type f); do
            printf -- "${RUNNING}" | grep -q "${PRIVILEGED}" && printf "OK:
'${PRIVILEGED}' found in auditing rules.\n" || printf "Warning:
'${PRIVILEGED}' not found in running configuration.\n"
        done
    done \
    || printf "ERROR: Variable 'RUNNING' is unset.\n"
}
```

Verify that all output is OK.

### Special mount points

If there are any special mount points that are not visible by default from `findmnt` as per the above audit, said file systems would have to be manually audited.

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor the use of privileged commands.

Example:

```
# {
    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

## **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.

### **NIST SP 800-53 Rev. 5:**

- AU-3
- AU-3(1)

### **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>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><br>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, M1047 |

### *5.2.3.7 Ensure unsuccessful file access attempts are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Monitor for unsuccessful attempts to access files. The following parameters are associated with system calls that control files:

- creation - `creat`
- opening - `open` , `openat`
- truncation - `truncate` , `ftruncate`

An audit log record will only be written if all of the following criteria is met for the user when trying to access a file:

- a non-privileged user (`auid>=UID_MIN`)
- is not a Daemon event (`auid=4294967295/unset/-1`)
- if the system call returned EACCES (permission denied) or EPERM (some other permanent error associated with the specific system call)

#### **Rationale:**

Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

## Audit:

### 64 Bit systems

#### **On disk configuration**

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&& / -F *arch=b[2346]{2}/ \
&& / -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[2346]{2}/ \
&& / -F *auid!=unset/ || / -F *auid!=-1/ || / -F *auid!=4294967295/ ) \
&& / -F *auid>=${UID_MIN}/ \
&& / -F *exit==EACCES/ || / -F *exit==EPERM/ ) \
&& / -S/ \
&& /creat/ \
&& /open/ \
&& /truncate/ \
&& / key= *[!~]* *$/ || / -k *[!~]* *$/)" \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit==EACCES -F auid>=1000
-F auid!=-1 -F key=access
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit==EPERM -F auid>=1000 -
F auid!=-1 -F key=access
-a always,exit -F arch=b32 -S open,truncate,ftruncate,creat,openat -F exit==EACCES -F auid>=1000
-F auid!=-1 -F key=access
-a always,exit -F arch=b32 -S open,truncate,ftruncate,creat,openat -F exit==EPERM -F auid>=1000 -
F auid!=-1 -F key=access
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor unsuccessful file access attempts.

### **64 Bit systems**

Example:

```
# {
UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit==EACCES -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit==EPERM -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit==EACCES -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit==EPERM -F auid>=${UID_MIN} -F auid!=unset -k access
" >> /etc/audit/rules.d/50-access.rules || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **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><br>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><br>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       |

### *5.2.3.8 Ensure events that modify user/group information are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Record events affecting the modification of user or group information, including that of passwords and old passwords if in use.

- /etc/group - system groups
- /etc/passwd - system users
- /etc/gshadow - encrypted password for each group
- /etc/shadow - system user passwords
- /etc/security/opasswd - storage of old passwords if the relevant PAM module is in use

The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier "identity" in the audit log file.

#### **Rationale:**

Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/etc/group/ \
||/etc/passwd/ \
||/etc/gshadow/ \
||/etc/shadow/ \
||/etc/security/opasswd/) \
&& / +p *wa/ \
&&(/ key= *[!-~]* *$/ ||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

### Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/etc/group/ \
||/etc/passwd/ \
||/etc/gshadow/ \
||/etc/shadow/ \
||/etc/security/opasswd/) \
&& / +p *wa/ \
&&(/ key= *[!-~]* *$/ ||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify user/group information.

Example:

```
# printf "
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
" >> /etc/audit/rules.d/50-identity.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **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><br/> 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><br/> 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       |

### *5.2.3.9 Ensure discretionary access control permission modification events are collected (Automated)*

#### **Profile Applicability:**

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

#### **Description:**

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes.

The following commands and system calls effect the permissions, ownership and various attributes of files.

- chmod
- fchmod
- fchmodat
- chown
- fchown
- fchownat
- lchown
- setxattr
- lsetxattr
- fsetxattr
- removexattr
- lremovexattr
- fremovexattr

In all cases, an audit record will only be written for non-system user ids and will ignore Daemon events. All audit records will be tagged with the identifier "perm\_mod."

#### **Rationale:**

Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
    && / -F *arch=b[2346]{2}/ \
    && / -F *auid!=unset||| -F *auid!=-1||| -F *auid!=4294967295/) \
    && / -S/ \
    && / -F *auid>=${UID_MIN}/ \
    && (/chmod|||fchmod7|||fchmodat/ \
      ||chown|||fchown|||fchownat|||lchown/ \
      ||setxattr|||lsetxattr|||fsetxattr/ \
      ||removexattr|||lremovexattr|||fremovexattr/) \
    && (/ key= *[!~]* *$||| -k *[!~]* *$/) "/etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F auid!=unset -F
key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F auid!=unset -F
key=perm_mod
-a always,exit -F arch=b64 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr
-F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr
-F auid>=1000 -F auid!=unset -F key=perm_mod
```

#### *Running configuration*

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
    && / -F *arch=b[2346]{2}/ \
    && / -S/ \
    && / -F *auid>=${UID_MIN}/ \
    && (/chmod|||fchmod7|||fchmodat/ \
      ||chown|||fchown|||fchownat|||lchown/ \
      ||setxattr|||lsetxattr|||fsetxattr/ \
      ||removexattr|||lremovexattr|||fremovexattr/) \
    && (/ key= *[!~]* *$||| -k *[!~]* *$/) \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F auid!=-1 -F
key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F auid!=-1 -F
key=perm_mod
-a always,exit -F arch=b64 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr
-F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr
-F auid>=1000 -F auid!=-1 -F key=perm_mod
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor discretionary access control permission modification events.

### **64 Bit systems**

**Example:**

```
# {
UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=${UID_MIN} -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lcown,fchownat -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=${UID_MIN} -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lcown,fchown,lcown,fchownat -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
" >> /etc/audit/rules.d/50-perm_mod.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **References:**

1. NIST SP 800-53 Rev. 5: AU-3, CM-6
2. NIST SP 800-53 Revision 4 :: AU-12 c

## **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.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238258  
Rule ID: SV-238258r653949\_rule  
STIG ID: UBTU-20-010142  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>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><br>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, M1047 |

### *5.2.3.10 Ensure successful file system mounts are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Monitor the use of the `mount` system call. The `mount` (and `umount`) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the `mount` system call is used by a non-privileged user

#### **Rationale:**

It is highly unusual for a non privileged user to `mount` file systems to the system. While tracking `mount` commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful `open`, `creat` and `truncate` system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
    && / -F *arch=b[234]{2}/ \
    && / -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[234]{2}/ \
    && / -F *auid!=unset/ || / -F *auid!=-1/ || / -F *auid!=4294967295/ ) \
    && / -F *auid>=${UID_MIN}/ \
    && / -S/ \
    && /mount/ \
    && ( key= *[!-~]* *$/ || / -k *[!-~]* *$/ ) " \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid==1 -F key=mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid==1 -F key=mounts
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful file system mounts.

### **64 Bit systems**

Example:

```
# {
UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b32 -S mount -F auid>=$UID_MIN -F auid!=unset -k
mounts
-a always,exit -F arch=b64 -S mount -F auid>=$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
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **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               | <b>8.5 Collect Detailed Audit Logs</b><br>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><br>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            | TA0010  | M1034       |

### *5.2.3.11 Ensure session initiation information is collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Monitor session initiation events. The parameters in this section track changes to the files associated with session events.

- `/var/run/utmp` - tracks all currently logged in users.
- `/var/log/wtmp` - file tracks logins, logouts, shutdown, and reboot events.
- `/var/log/btmp` - keeps track of failed login attempts and can be read by entering the command `/usr/bin/last -f /var/log/btmp`.

All audit records will be tagged with the identifier "session."

#### **Rationale:**

Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/\/var\/run\/utmp/ \
||/\/var\/log\/wtmp/ \
||/\/var\/log\/btmp/) \
&&/ +-p *wa/ \
&&(/ key= *[^-~]* *$||/ -k *[^-~]* *$/) ' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
```

### Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/\/var\/run\/utmp/ \
||/\/var\/log\/wtmp/ \
||/\/var\/log\/btmp/) \
&&/ +-p *wa/ \
&&(/ key= *[^-~]* *$||/ -k *[^-~]* *$/) '
```

Verify the output matches:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
```

### Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor session initiation information.

Example:

```
# printf "
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
" >> /etc/audit/rules.d/50-session.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **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.

## **NIST SP 800-53 Rev. 5:**

- AU-3
- AU-3(1)

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238315  
Rule ID: SV-238315r654120  
STIG ID: UBTU-20-010277  
Severity: CAT II

Vul ID: V-238316  
Rule ID: SV-238316r880873  
STIG ID: UBTU-20-010278  
Severity: CAT II

Vul ID: V-238317  
Rule ID: SV-238317r654126  
STIG ID: UBTU-20-010279  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <p><b>8.5 Collect Detailed Audit Logs</b><br/> 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><br/> 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><br/> 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       |

### *5.2.3.12 Ensure login and logout events are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Monitor login and logout events. The parameters below track changes to files associated with login/logout events.

- `/var/log/lastlog` - maintain records of the last time a user successfully logged in.
- `/var/run/faillock` - directory maintains records of login failures via the `pam_faillock` module.

#### **Rationale:**

Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

#### **Audit:**

##### **On disk configuration**

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/\/var\/log\/lastlog/ \
| /\/var\/run\/faillock/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
```

##### **Running configuration**

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/\/var\/log\/lastlog/ \
| /\/var\/run\/faillock/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
```

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor login and logout events.

Example:

```
# printf "
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
" >> /etc/audit/rules.d/50-login.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **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.

### **NIST SP 800-53 Rev. 5:**

- AU-3
- AU-3(1)

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <p><b>8.5 Collect Detailed Audit Logs</b><br/> 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><br/> Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.</p>                                                                                                                 |      | ●    | ●    |
| v7               | <p><b>16.11 Lock Workstation Sessions After Inactivity</b><br/> Automatically lock workstation sessions after a standard period of inactivity.</p>                                                                                                                                                      | ●    | ●    | ●    |
| v7               | <p><b>16.13 Alert on Account Login Behavior Deviation</b><br/> 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       |

### *5.2.3.13 Ensure file deletion events by users are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for:

- `unlink` - remove a file
- `unlinkat` - remove a file attribute
- `rename` - rename a file
- `renameat` rename a file attribute system calls and tags them with the identifier "delete".

#### **Rationale:**

Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
    &&/ -F *arch=b[2346]{2}/ \
    &&(/ -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[2346]{2}/ \
    &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -S/ \
    &&(/unlink/||/rename/||/unlinkat/||/renameat/) \
    &&(/ key= *[!-~]* *$/|/ -k *[!-~]* *$/) \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F auid>=1000 -
F auid!=-1 -F key=delete
-a always,exit -F arch=b32 -S unlink,rename,unlinkat,renameat -F auid>=1000 -
F auid!=-1 -F key=delete
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor file deletion events by users.

### **64 Bit systems**

Example:

```
# {
UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F
auid>=${UID_MIN} -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S rename,unlink,unlinkat,renameat -F
auid>=${UID_MIN} -F auid!=unset -F key=delete
" >> /etc/audit/rules.d/50-delete.rules || printf "ERROR: Variable 'UID_MIN'
is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

### **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               | <b>8.5 Collect Detailed Audit Logs</b><br>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><br>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  | M1047       |

### *5.2.3.14 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Monitor AppArmor, an implementation of mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/apparmor/ and /etc/apparmor.d/ directories.

**Note:** If a different Mandatory Access Control method is used, changes to the corresponding directories should be audited.

#### **Rationale:**

Changes to files in the /etc/apparmor/ and /etc/apparmor.d/ directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

#### **Audit:**

##### **On disk configuration**

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&& (/etc/apparmor/ \
| /etc/apparmor.d/) \
&& / +p *wa/ \
&& (/ key= *[!~-]* *$/||/ -k *[!~-]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
```

##### **Running configuration**

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&& (/etc/apparmor/ \
| /etc/apparmor.d/) \
&& / +p *wa/ \
&& (/ key= *[!~-]* *$/||/ -k *[!~-]* *$/)'
```

Verify the output matches:

```
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
```

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the system's Mandatory Access Controls.

Example:

```
# printf "
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
" >> /etc/audit/rules.d/50-MAC-policy.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **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><br/> 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><br/> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.</p>      |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0004  | M1022       |

*5.2.3.15 Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

The operating system must generate audit records for successful/unsuccessful uses of the `chcon` command.

**Rationale:**

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:

### 64 Bit systems

#### ***On disk configuration***

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/chcon/ \
    &&(/ key= *[!~-]* *$/|/ -k *[!~-]* *$/) " /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset
-k perm_chng
```

#### ***Running configuration***

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/chcon/ \
    &&(/ key= *[!~-]* *$/|/ -k *[!~-]* *$/) " \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F
auid==1 -F key=perm_chng
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `chcon` command.

### **64 Bit systems**

#### **Example:**

```
# {
  UID_MIN=$(awk '/^UID_MIN/{print $2}' /etc/login.defs)
  [ -n "$UID_MIN" ] && printf "
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-perm_chng.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **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               | <b>8.2 Collect Audit Logs</b><br>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><br>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  | M1022       |

*5.2.3.16 Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

The operating system must generate audit records for successful/unsuccessful uses of the `setfacl` command

**Rationale:**

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:

### 64 Bit systems

#### ***On disk configuration***

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/setfacl/ \
    &&(/ key= *[!~-]* *$/|/ -k *[!~-]* *$/) " /etc/audit/rules.d/*.rules ||
  printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=unset -k perm_chng
```

#### ***Running configuration***

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/setfacl/ \
    &&(/ key= *[!~-]* *$/|/ -k *[!~-]* *$/) \
    || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid==1 -F key=perm_chng
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `setfacl` command.

### **64 Bit systems**

#### **Example:**

```
# {
  UID_MIN=$(awk '/^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
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **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               | <b>8.2 Collect Audit Logs</b><br>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><br>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  | M1022       |

*5.2.3.17 Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

The operating system must generate audit records for successful/unsuccessful uses of the `chacl` command.

`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:

### 64 Bit systems

#### ***On disk configuration***

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/chacl/ \
    &&(/ key= *[!-~]* *$/|/ -k *[!-~]* *$/) " /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=unset
-k 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
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `chacl` command.

### **64 Bit systems**

#### **Example:**

```
# {
  UID_MIN=$(awk '/^UID_MIN/{print $2}' /etc/login.defs)
  [ -n "$UID_MIN" ] && printf "
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-perm_chng.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **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               | <b>8.2 Collect Audit Logs</b><br>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><br>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  | M1022       |

*5.2.3.18 Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

The operating system must generate audit records for successful/unsuccessful uses of the `usermod` command.

**Rationale:**

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:

### 64 Bit systems

#### ***On disk configuration***

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/sbin/usermod/ \
    &&(/ key= *[!-~]* *$/|/ -k *[!-~]* *$/) " /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=unset -k usermod
```

#### ***Running configuration***

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/sbin/usermod/ \
    &&(/ key= *[!-~]* *$/|/ -k *[!-~]* *$/) " \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid==1 -F key=usermod
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `usermod` command.

### **64 Bit systems**

#### **Example:**

```
# {
  UID_MIN=$(awk '/^UID_MIN/{print $2}' /etc/login.defs)
  [ -n "$UID_MIN" ] && printf "
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k usermod
" >> /etc/audit/rules.d/50-usermod.rules || printf "ERROR: Variable 'UID_MIN'
is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **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><br/>           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><br/>           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       |

### *5.2.3.19 Ensure kernel module loading unloading and modification is collected (Automated)*

#### **Profile Applicability:**

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

#### **Description:**

Monitor the loading and unloading of kernel modules. All the loading / listing / dependency checking of modules is done by `kmod` via symbolic links.

The following system calls control loading and unloading of modules:

- `init_module` - load a module
- `finit_module` - load a module (used when the overhead of using cryptographically signed modules to determine the authenticity of a module can be avoided)
- `delete_module` - delete a module
- `create_module` - create a loadable module entry
- `query_module` - query the kernel for various bits pertaining to modules

Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of `modules`.

#### **Rationale:**

Monitoring the use of all the various ways to manipulate kernel modules could provide system administrators with evidence that an unauthorized change was made to a kernel module, possibly compromising the security of the system.

## Audit:

### 64 Bit systems

#### ***On disk configuration***

Run the following commands to check the on disk rules:

```
# {
awk '/^ *-a *always,exit/ \
&& / -F *arch=b[2346]{2}/ \
&&(/ -F auid!=unset/||/ -F auid!=-1/||/ -F auid!=4294967295/) \
&& / -S/ \
&&(/init_module/ \
||/finit_module/ \
||/delete_module/ \
||/create_module/ \
||/query_module/) \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules

UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&& / -F *auid>=${UID_MIN}/ \
&& / -F *perm=x/ \
&& / -F *path=/usr/bin/kmod/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S init_module,finit_module,delete_module,create_module,query_module -
F auid>=1000 -F auid!=unset -k kernel_modules
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -k kernel_modules
```

#### ***Running configuration***

Run the following command to check loaded rules:

```
# {
auditctl -l | awk '/^ *-a *always,exit/ \
&& / -F *arch=b[2346]{2}/ \
&&(/ -F auid!=unset/||/ -F auid!=-1/||/ -F auid!=4294967295/) \
&& / -S/ \
&&(/init_module/ \
||/finit_module/ \
||/delete_module/ \
||/create_module/ \
||/query_module/) \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' 

UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&& / -F *auid>=${UID_MIN}/ \
&& / -F *perm=x/ \
&& / -F *path=/usr/bin/kmod/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S create_module,init_module,delete_module,query_module,finit_module -F auid>=1000 -F auid!=--1 -F key=kernel_modules  
-a always,exit -S all -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=--1 -F key=kernel_modules
```

## Symlink audit

Audit if the symlinks that kmod accepts is indeed pointing at it:

```
# S_LINKS=$(ls -l /usr/sbin/lsmod /usr/sbin/rmmod /usr/sbin/insmod /usr/sbin/modinfo /usr/sbin/modprobe /usr/sbin/depmod | grep -v " -> ./bin/kmod" || true) \  
&& if [[ "$S_LINKS" != "" ]]; then printf "Issue with symlinks: ${S_LINKS}\n"; else printf "OK\n"; fi
```

Verify the output states OK. If there is a symlink pointing to a different location it should be investigated.

## Remediation:

### Create audit rules

Edit or create a file in the /etc/audit/rules.d/ directory, ending in .rules extension, with the relevant rules to monitor kernel module modification.

### 64 Bit systems

#### Example:

```
# {  
UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)  
[ -n "$UID_MIN" ] && printf "  
-a always,exit -F arch=b64 -S init_module,finit_module,delete_module,create_module,query_module -F auid>=${UID_MIN} -F auid!=unset -k kernel_modules  
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=${UID_MIN} -F auid!=unset -k kernel_modules  
" >> /etc/audit/rules.d/50-kernel_modules.rules || printf "ERROR: Variable 'UID_MIN' is unset.\n"  
}
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n";  
fi
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3, CM-6
2. NIST SP 800-53 Revision 4 :: AU-12 c

## **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.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238295  
Rule ID: SV-238295r654060\_rule  
STIG ID: UBTU-20-010179  
Severity: CAT II

Vul ID: V-238297  
Rule ID: SV-238297r654066\_rule  
STIG ID: UBTU-20-010181  
Severity: CAT II

Vul ID: V-238318  
Rule ID: SV-238318r654129\_rule  
STIG ID: UBTU-20-010296  
Severity: CAT II

Vul ID: V-238319  
Rule ID: SV-238319r654132\_rule  
STIG ID: UBTU-20-010297  
Severity: CAT II

## **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><br>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><br>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       |

DRAFT

### *5.2.3.20 Ensure successful and unsuccessful uses of the su command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the su command.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify the Ubuntu operating system generates audit records upon successful/unsuccessful attempts to use the "su" command.

Check the configured audit rules with the following commands:

```
# auditctl -l | grep '/bin/su'  
  
-a always,exit -F path=/bin/su -F perm=x -F auid>=1000 -F auid!=4294967295 -k  
privileged-priv_change
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the Ubuntu operating system to generate audit records when successful/unsuccessful attempts to use the "su" command occur.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/bin/su -F perm=x -F auid>=1000 -F  
auid!=4294967295 -k privileged-priv_change" >> "/etc/audit/rules.d/50-  
stig.rules"
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238252  
Rule ID: SV-238252r653931\_rule  
STIG ID: UBTU-20-010136  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.21 Ensure successful and unsuccessful uses of the chfn command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the chfn command.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify the Ubuntu operating system generates audit records upon successful/unsuccessful attempts to use the "chfn" command.

Check the configured audit rules with the following commands:

```
# auditctl -l | grep '/usr/bin/chfn'  
  
-a always,exit -F path=/usr/bin/chfn -F perm=x -F auid>=1000 -F auid!=--1 -k  
privileged-chfn
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "chfn" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/usr/bin/chfn -F perm=x -F auid>=1000  
-F auid!=4294967295 -k privileged-chfn" >> /etc/audit/rules.d/50-stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238253  
Rule ID: SV-238253r653934\_rule  
STIG ID: UBTU-20-010137  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.22 Ensure successful and unsuccessful uses of the ssh-agent command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the ssh-agent command.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "ssh-agent" command.  
Check the configured audit rules with the following commands:

```
# auditctl -l | grep '/usr/bin/ssh-agent'  
  
-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F auid!=--1  
-k privileged-ssh
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "ssh-agent" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F  
auid>=1000 -F auid!=4294967295 -k privileged-ssh" >> /etc/audit/rules.d/50-  
stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238256  
Rule ID: SV-238256r653943\_rule  
STIG ID: UBTU-20-010140  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.23 Ensure successful and unsuccessful uses of the ssh-keysign command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the ssh-keysign command.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "ssh-keysign" command.  
Check the configured audit rules with the following commands:

```
# auditctl -l | grep ssh-keysign  
  
-a always,exit -F path=/usr/lib/openssh/ssh-keysign -F perm=x -F auid>=1000 -  
F auid!=--1 -k privileged-ssh
```

If the command does not return lines that match the example or the lines are commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "ssh-keysign" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/usr/lib/openssh/ssh-keysign -F  
perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-ssh" >>  
/etc/audit/rules.d/50-stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238257  
Rule ID: SV-238257r653946\_rule  
STIG ID: UBTU-20-010141  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.24 Ensure successful and unsuccessful attempts to use the fdisk command are recorded (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records when successful/unsuccessful attempts to use the fdisk command.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify the Ubuntu operating system is configured to audit the execution of the module management program "fdisk".

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep fdisk  
-w /bin/fdisk -p x -k module
```

If the command does not return a line, or the line is commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the Ubuntu operating system to audit the execution of the partition management program "fdisk".

Add or update the following rule in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-w /bin/fdisk -p x -k fdisk" >> /etc/audit/rules.d/50-  
stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

#### **References:**

1. NIST SP 800-53 Revision 4 :: AU-12 c

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238320  
Rule ID: SV-238320r654135\_rule  
STIG ID: UBTU-20-010298  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.25 Ensure successful and unsuccessful uses of the sudo command are recorded (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the sudo command.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "sudo" command.

Check the configured audit rules with the following command:

```
# auditctl -l | grep /usr/bin/sudo  
  
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=--1 -k  
priv_cmd
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "sudo" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000  
-F auid!=4294967295 -k priv_cmd" >> /etc/audit/rules.d/50-stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238277  
Rule ID: SV-238277r654006\_rule  
STIG ID: UBTU-20-010161  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.26 Ensure successful and unsuccessful attempts to use the pam\_timestamp\_check command are recorded (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the pam\_timestamp\_check command.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "pam\_timestamp\_check" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w pam_timestamp_check  
  
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000  
-F auid!=--1 -k privileged-pam_timestamp_check
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "pam\_timestamp\_check" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/usr/sbin/pam_timestamp_check -F  
perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-pam_timestamp_check"  
>> /etc/audit/rules.d/50-stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238294  
Rule ID: SV-238294r654057\_rule  
STIG ID: UBTU-20-010178  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.27 Ensure successful and unsuccessful attempts to use the sudoedit command are recorded (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the sudoedit command.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "sudoedit" command.

Check the configured audit rules with the following commands:

```
# auditctl -l | grep /usr/bin/sudoedit  
  
-a always,exit -F path=/usr/bin/sudoedit -F perm=x -F auid>=1000 -F auid!=--1  
-k priv_cmd
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "sudoedit" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules":

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/usr/bin/sudoedit -F perm=x -F  
auid>=1000 -F auid!=4294967295 -k priv_cmd" >> /etc/audit/rules.d/50-  
stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238278  
Rule ID: SV-238278r654009\_rule  
STIG ID: UBTU-20-010162  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.28 Ensure successful and unsuccessful attempts to use the crontab command are recorded (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the crontab command.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "crontab" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w crontab  
  
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F auid!=-1 -  
k privileged-crontab
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "crontab" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/usr/bin/crontab -F perm=x -F  
auid>=1000 -F auid!=4294967295 -k privileged-crontab" >>  
/etc/audit/rules.d/50-stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238293  
Rule ID: SV-238293r654054\_rule  
STIG ID: UBTU-20-010177  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.29 Ensure successful and unsuccessful attempts to use the chsh command are recorded (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the chsh command.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "chsh" command.

Check the configured audit rules with the following commands:

```
# auditctl -l | grep chsh  
  
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=--1 -k  
priv_cmd
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chsh" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000  
-F auid!=4294967295 -k priv_cmd" >> /etc/audit/rules.d/50-stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238279  
Rule ID: SV-238279r654012\_rule  
STIG ID: UBTU-20-010163  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.30 Ensure successful and unsuccessful attempts to use the chage command are recorded (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the chage command

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "chage" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w chage  
  
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=--1 -k  
privileged-chage
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "chage" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

#### *Example:*

```
# printf '\n%s' "-a always,exit -F path=/usr/bin/chage -F perm=x -F  
auid>=1000 -F auid!=4294967295 -k privileged-chage" >> /etc/audit/rules.d/50-  
stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238291  
Rule ID: SV-238291r654048\_rule  
STIG ID: UBTU-20-010175  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.31 Ensure successful and unsuccessful attempts to use the newgrp command are recorded (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the newgrp command.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "newgrp" command.

Check the configured audit rules with the following commands:

```
# auditctl -l | grep newgrp  
  
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=--1 -k  
priv_cmd
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "newgrp" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/usr/bin/newgrp -F perm=x -F  
auid>=1000 -F auid!=4294967295 -k priv_cmd" >> /etc/audit/rules.d/50-  
stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238280  
Rule ID: SV-238280r654015\_rule  
STIG ID: UBTU-20-010164  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.32 Ensure successful and unsuccessful attempts to use the gpasswd command are recorded (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the gpasswd command

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "gpasswd" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w gpasswd  
  
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F auid!=-1 -  
k privileged-gpasswd
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "gpasswd" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F  
auid>=1000 -F auid!=4294967295 -k privileged-gpasswd" >>  
/etc/audit/rules.d/50-stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238290  
Rule ID: SV-238290r654045\_rule  
STIG ID: UBTU-20-010174  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.33 Ensure successful and unsuccessful attempts to use the unix\_update command are recorded (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the unix\_update command

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "unix\_update" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w unix_update  
  
-a always,exit -F path=/sbin/unix_update -F perm=x -F auid>=1000 -F auid!=--1  
-k privileged-unix-update
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "unix\_update" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/sbin/unix_update -F perm=x -F  
auid>=1000 -F auid!=4294967295 -k privileged-unix-update" >>  
/etc/audit/rules.d/50-stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238289  
Rule ID: SV-238289r654042\_rule  
STIG ID: UBTU-20-010173  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.34 Ensure successful and unsuccessful attempts to use the apparmor\_parser command are recorded (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the apparmor\_parser command.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify the Ubuntu operating system generates an audit record upon successful/unsuccessful attempts to use the "apparmor\_parser" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep apparmor_parser  
  
-a always,exit -F path=/sbin/apparmor_parser -F perm=x -F auid>=1000 -F  
auid!=--1 -k perm_chng
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "apparmor\_parser" command.

Add or update the following rules in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/sbin/apparmor_parser -F perm=x -F  
auid>=1000 -F auid!=4294967295 -k perm_chng" >> /etc/audit/rules.d/50-  
stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238282  
Rule ID: SV-238282r654021\_rule  
STIG ID: UBTU-20-010166  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### *5.2.3.35 Ensure successful and unsuccessful attempts to use the passwd command are recorded (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the passwd command

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "passwd" command.

Check the currently configured audit rules with the following command:

```
# auditctl -l | grep -w passwd  
  
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=--1 -k  
privileged-passwd
```

If the command does not return a line that matches the example or the line is commented out, this is a finding.

**Note:** The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

#### **Remediation:**

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "passwd" command.

Add or update the following rule in the "/etc/audit/rules.d/50-stig.rules" file:

*Example:*

```
# printf '\n%s' "-a always,exit -F path=/usr/bin/passwd -F perm=x -F  
auid>=1000 -F auid!=4294967295 -k privileged-passwd" >>  
/etc/audit/rules.d/50-stig.rules
```

To reload the rules file, issue the following command:

```
# augenrules --load
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-12 c

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238288  
Rule ID: SV-238288r654039\_rule  
STIG ID: UBTU-20-010172  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 Collect Audit Logs</b><br>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><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | ●    | ●    | ●    |

### 5.2.3.36 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:**

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>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><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |      | ●    | ●    |

### 5.2.3.37 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  
" >> /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  
required 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               | <p><b>3.3 Configure Data Access Control Lists</b><br/> Configure data access control lists based on a 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>8.5 Collect Detailed Audit Logs</b><br/> 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><br/> Ensure that local logging has been enabled on all systems and networking devices.</p>                                                                                                                                                                         | ●    | ●    | ●    |
| v7               | <p><b>6.3 Enable Detailed Logging</b><br/> 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       |

#### **5.2.4 Configure auditd file access**

Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events.

DRAFT

## *5.2.4.1 Ensure the audit log directory is 0750 or more restrictive (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 command to verify that the audit log directory has a mode of 0750 or less permissive:

```
# stat -Lc "%n %a" "$(dirname $(awk -F"="/^\s*log_file/ {print $2}" /etc/audit/auditd.conf))" | grep -Pv -- '^h*\H+\h+([0,5,7][0,5]0)'
```

Nothing should be returned

### **Remediation:**

Run the following command to configure the audit log directory to have a mode of "0750" or less permissive:

```
# chmod g-w,o-rwx "$(dirname $(awk -F"="/^\s*log_file/ {print $2}" /etc/audit/auditd.conf))"
```

### **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><br/> Configure data access control lists based on a 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><br/> 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  | M1047       |

## *5.2.4.2 Ensure audit log files are mode 0640 or more restrictive (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 audit log files have mode 0640 or less permissive:

```
# [ -f /etc/audit/auditd.conf ] && find "$(dirname $(awk -F "=" '/^s*log_file/ {print $2}' /etc/audit/auditd.conf | xargs))" -type f -perm /0137 -exec stat -Lc "%n %#a" {} +
```

Nothing should be returned

### **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><br/> Configure data access control lists based on a 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><br/> 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  | M1047       |

### *5.2.4.3 Ensure audit log files are mode 0600 or more restrictive (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must be configured so that audit log files are not read or write-accessible by unauthorized users.

#### **Rationale:**

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit operating system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028

#### **Audit:**

Verify that the audit log files have a mode of "0600" or less permissive.  
Determine where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
  
log_file = /var/log/audit/audit.log
```

Using the path of the directory containing the audit logs, determine if the audit log files have a mode of "0600" or less by using the following command:

```
# stat -c "%n %a" /var/log/audit/*  
  
/var/log/audit/audit.log 600
```

If the audit log files have a mode more permissive than "0600", this is a finding.

#### **Remediation:**

Configure the audit log files to have a mode of "0600" or less permissive.  
Determine where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
  
log_file = /var/log/audit/audit.log
```

Using the path of the directory containing the audit logs, configure the audit log files to have a mode of "0600" or less permissive by using the following command:

```
# chmod 0600 /var/log/audit/*
```

## References:

1. NIST SP 800-53 :: AU-9

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238245  
Rule ID: SV-238245r653910\_rule  
STIG ID: UBTU-20-010122  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

## *5.2.4.4 Ensure only authorized users own audit log files (Automated)*

### **Profile Applicability:**

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

### **Description:**

Audit log files contain information about the system and system activity.

### **Rationale:**

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

### **Audit:**

Run the following command to verify audit log files are owned by the `root` user:

```
# [ -f /etc/audit/auditd.conf ] && find "$(dirname $(awk -F "=" '/^log_file/ {print $2}' /etc/audit/auditd.conf | xargs))" -type f ! -user root -exec stat -Lc "%n %U" {} +
```

Nothing should be returned

### **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 "=" '/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
2. NIST SP 800-53 :: AU-9

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238246  
Rule ID: SV-238246r653913\_rule  
STIG ID: UBTU-20-010123  
Severity: CAT II

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>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, M1047 |

## *5.2.4.5 Ensure only authorized groups own audit log files (Automated)*

### **Profile Applicability:**

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

### **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 -- '(amd)'
```

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*#.*)?.*$/{log_group = adm}\\1/' /etc/audit/auditd.conf
```

Run the following command to restart the audit daemon to reload the configuration file:

```
# systemctl restart auditd
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3
2. NIST SP 800-53 Revision 4 :: AU-9

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238247  
Rule ID: SV-238247r653916\_rule  
STIG ID: UBTU-20-010124  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>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> |
|------------------------------------|----------------|--------------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007         | M1047              |

DRAFT

## *5.2.4.6 Ensure audit configuration files are 640 or more restrictive (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 have mode 640 or more restrictive and are owned by the root user and root group:

```
# find /etc/audit/ -type f \(-name '*.conf' -o -name '*.rules'\) -exec stat -Lc "%n %a" {} + | grep -Pv -- '^\\h*\\H+\\h*([0,2,4,6][0,4]0)\\h*$'
```

Nothing should be returned

### **Remediation:**

Run the following command to remove more permissive mode than 0640 from the audit configuration files:

```
# find /etc/audit/ -type f \(-name '*.conf' -o -name '*.rules'\) -exec chmod u-x,g-wx,o-rwx {} +
```

### **References:**

1. NIST SP 800-53 Rev. 5: AU-3
2. NIST SP 800-53 :: AU-12 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238249  
Rule ID: SV-238249r653922\_rule  
STIG ID: UBTU-20-010133  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>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  | M1047       |

## *5.2.4.7 Ensure only authorized users own audit configuration files (Automated)*

### **Profile Applicability:**

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

### **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 commands 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  
# find /etc/audit/rules.d/ -type f ! -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 {} +  
find /etc/audit/rules.d/ -type f ! -user root -exec chown root {} +
```

### **References:**

1. NIST SP 800-53 Rev. 5: AU-3
2. NIST SP 800-53 Revision 5 :: AU-12 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238250  
Rule ID: SV-238250r653925\_rule  
STIG ID: UBTU-20-010134  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>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  | M1047       |

## *5.2.4.8 Ensure only authorized groups own audit configuration files (Automated)*

### **Profile Applicability:**

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

### **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 commands 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  
# find /etc/audit/rules.d/ -type f ! -group root
```

Nothing should be returned

### **Remediation:**

Run the following commands to change group to root:

```
# find /etc/audit/ -type f \(-name '*.conf' -o -name '*.rules'\) ! -group root -exec chgrp root {} +  
# find /etc/audit/rules.d -type f ! -group root -exec chgrp root {} +
```

### **References:**

1. NIST SP 800-53 Rev. 5: AU-3
2. NIST SP 800-53 Revision 5 :: AU-12 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238251  
Rule ID: SV-238251r653928\_rule  
STIG ID: UBTU-20-010135  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>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  | M1047       |

## 5.2.4.9 Ensure audit tools are 755 or more restrictive (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 755 or more restrictive:

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

{
    l_output="" l_output2="" l_count="0"
    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/audispd" "/sbin/augenrules")
    for l_fname in "${a_audit_tools[@]}"; do
        if [ -e "$l_fname" ]; then
            (( l_count++ ))
            l_mode=$(stat -Lc %#a "$l_fname")
            if [ $(( "$l_mode" & "$l_perm_mask" )) -gt 0 ]; then
                l_output2="$l_output2\n - Directory: \"$l_fname\" is mode: \"$l_mode\""
                (should be mode: \"$l_maxperm\" or more restrictive)"
            fi
        fi
    done
    if [ -z "$l_output2" ]; then
        if [ "$l_count" -gt "0" ]; then
            l_output=" - All audit tools files are mode: \"$l_maxperm\" or more
restrictive"
        else
            l_output=" - No audit tools files exist"
        fi
    fi
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n  ** PASS **\n$l_output"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n$l_output2"
    fi
}
```

## **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               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>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  | M1047       |

### *5.2.4.10 Ensure only authorized users own 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 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 owned by the root user:

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

{
    l_output="" l_output2="" l_count="0"
    l_owner="root"
    a_audit_tools=( "/sbin/auditctl" "/sbin/aureport" "/sbin/ausearch" "/sbin/autrace"
    "/sbin/auditd" "/sbin/audispd" "/sbin/augenrules")
    for l_fname in "${a_audit_tools[@]}"; do
        if [ -e "$l_fname" ]; then
            (( l_count++ ))
            l_file_owner=$(stat -Lc '%U' "$l_fname")"
            if [[ ! "$l_file_owner" =~ $l_owner\s*$ ]]; then
                l_output2="$l_output2\n - file: \"$l_fname\" is owned by:
\"$l_file_owner\" (should be owned by: \"${l_owner}/|/ or }\")"
            fi
        fi
    done
    if [ -z "$l_output2" ]; then
        if [ "$l_count" -gt "0" ]; then
            l_output=" - All audit tools files are owned by: \"${l_owner}/|/ or }\"
"
        else
            l_output=" - No audit tools files exist"
        fi
    fi
    unset a_audit_tools
    # If the tests produce no failing output, we pass
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n  ** PASS **\n$l_output"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n$l_output2"
    fi
}
```

## 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><br/> Configure data access control lists based on a 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><br/> 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  | M1047       |

### *5.2.4.11 Ensure only authorized groups own audit tools (Automated)*

#### **Profile Applicability:**

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

#### **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:

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

{
    l_output="" l_output2="" l_count="0"
    l_group_owner="root"
    a_audit_tools=(/sbin/auditctl "/sbin/aureport" "/sbin/ausearch"
    "/sbin/autrace" "/sbin/auditd" "/sbin/audispd" "/sbin/augenrules")
    for l_fname in "${a_audit_tools[@]}"; do
        if [ -e "$l_fname" ]; then
            (( l_count++ ))
            l_file_group_owner=$(stat -Lc '%G' "$l_fname")
            if [[ ! "$l_file_group_owner" =~ ${l_group_owner}\s*$ ]]; then
                l_output2="$l_output2\n - file: \"$l_fname\" is owned by:
\"$l_file_group_owner\" (should be owned by: \"${l_group_owner}/|/ or \")"
            fi
        fi
    done
    if [ -z "$l_output2" ]; then
        if [ "$l_count" -gt "0" ]; then
            l_output=" - All audit tools files are owned by:
\"${l_group_owner}/|/ or \\""
        else
            l_output=" - No audit tools files exist"
        fi
    fi
    unset a_audit_tools
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n  ** PASS **\n$l_output"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n$l_output2"
    fi
}
```

## Remediation:

Run the following command to remove more permissive mode from the audit tools:

```
# chmod go-w /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace
/sbin/auditd /sbin/augenrules
```

Run the following command to change owner and group of the audit tools to root user and group:

```
# chown root:root /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace
/sbin/auditd /sbin/augenrules
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3
2. NIST SP 800-53 Revision 5 :: AU-9

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238302  
Rule ID: SV-238302r654081\_rule  
STIG ID: UBTU-20-010201  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>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  | M1047       |

## 5.3 Filesystem Integrity Checking

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

DRAFT

### *5.3.1 Ensure AIDE is installed (Automated)*

#### **Profile Applicability:**

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

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Run the following commands to verify AIDE is installed:

```
# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n' aide  
aide-common  
  
aide      install ok installed      installed  
aide-common    install ok installed      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.

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238371  
Rule ID: SV-238371r880913\_rule  
STIG ID: UBTU-20-010450  
Severity: CAT II

**Note:** Required for AIDE based recommendations

## **CIS Controls:**

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

### *5.3.2 Ensure aide script to check file integrity is the default (Manual)*

#### **Profile Applicability:**

- STIG

#### **Description:**

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

#### **Rationale:**

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

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

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

#### **Audit:**

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

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

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

Fetch the SHA1 of the original script file:

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

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

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

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

## **Remediation:**

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

Download the original package to the /tmp dir:

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

Extract the aide script to its original place:

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

Copy it to the cron.daily directory:

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

## **References:**

1. NIST SP 800-53 Revision 5 :: SI-6 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238236  
Rule ID: SV-238236r653883\_rule  
STIG ID: UBTU-20-010074  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.1 Establish and Maintain a Secure Configuration Process</b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and 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>5.1 Establish Secure Configurations</b><br>Maintain documented, standard security configuration standards for all authorized operating systems and software.                                                                                                                                                                                                                                                       | ●    | ●    | ●    |

### 5.3.3 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|([^\#\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 --check
```

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

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

```
[Unit]
Description=Aide Check

[Service]
Type=simple
ExecStart=/usr/bin/aide.wrapper --config /etc/aide/aide.conf --check

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

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

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

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

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

Run the following commands:

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

# systemctl daemon-reload

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

## **References:**

1. <https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.service>
2. <https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.timer>
3. NIST SP 800-53 Rev. 5: AU-2

## **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><br>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><br>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       |

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

#### **Profile Applicability:**

- STIG

#### **Description:**

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

#### **Rationale:**

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

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

#### **Audit:**

Verify that Advanced Intrusion Detection Environment (AIDE) notifies the System Administrator when anomalies in the operation of any security functions are discovered with the following command:

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

If SILENTREPORTS is commented out, this is a finding.

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

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

#### **Remediation:**

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

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

## References:

1. NIST SP 800-53 Revision 5 :: SI-6 d
2. NIST SP 800-53 Revision 4 :: SI-6 d

## Additional Information:

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238358  
Rule ID: SV-238358r654249\_rule  
STIG ID: UBTU-20-010437  
Severity: CAT II

Vul ID: V-238372  
Rule ID: SV-238372r654318\_rule  
STIG ID: UBTU-20-010451  
Severity: CAT II

## CIS Controls:

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

### *5.3.5 Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

Attackers may replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

Audit tools should be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

#### **Audit:**

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

```
# grep -Ps -- '(\sbin\/(audit|au)\H*\b)' /etc/aide.conf /etc/aide/aide.conf  
/etc/aide.conf.d/*.*.conf /etc/aide/aide.conf.d/*
```

Verify the output includes:

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

## **Remediation:**

Add or update the following selection lines for to a file ending in `.conf` in the `/etc/aide/aide.conf.d/` or to `/etc/aide/aide.conf` to protect the integrity of the audit tools:

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

## **References:**

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

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

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007         | M1047              |

## **6 System Maintenance**

Recommendations in this section are intended as maintenance and are intended to be checked on a frequent basis to ensure system stability. Many recommendations do not have quick remediations and require investigation into the cause and best fix available and may indicate an attempted breach of system security.

DRAFT

## **6.1 System File Permissions**

This section provides guidance on securing aspects of system files and directories.

DRAFT

## *6.1.1 Ensure permissions on /etc/passwd are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/passwd` file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

### **Rationale:**

It is critical to ensure that the `/etc/passwd` file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### **Audit:**

Run the following command to verify `/etc/passwd` is mode 644 or more restrictive, `Uid is 0/root and Gid is 0/root`:

```
# stat -Lc "%n %a %u/%U %g/%G" /etc/passwd
/etc/passwd 644 0/root 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:**

`/etc/passwd 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               | <p><b>3.3 Configure Data Access Control Lists</b><br/> Configure data access control lists based on a 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><br/> 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       |

## *6.1.2 Ensure permissions on /etc/passwd- are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The /etc/passwd- file contains backup user account information.

### **Rationale:**

It is critical to ensure that the /etc/passwd- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### **Audit:**

Run the following command to verify /etc/passwd- is mode 644 or more restrictive, Uid is 0/root and Gid is 0/root:

```
# stat -Lc "%n %a %u/%U %g/%G" /etc/passwd-
/etc/passwd- 644 0/root 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:**

/etc/passwd- 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               | <p><b>3.3 Configure Data Access Control Lists</b><br/> Configure data access control lists based on a 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><br/> 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       |

### *6.1.3 Ensure permissions on /etc/group are configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `/etc/group` file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

#### **Rationale:**

The `/etc/group` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

#### **Audit:**

Run the following command to verify `/etc/group` is mode 644 or more restrictive, `Uid` is 0/root and `Gid` is 0/root:

```
# stat -Lc "%n %a %u/%U %g/%G" /etc/group
/etc/group 644 0/root 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:**

`/etc/group` 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               | <p><b>3.3 Configure Data Access Control Lists</b><br/> Configure data access control lists based on a 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><br/> 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       |

## *6.1.4 Ensure permissions on /etc/group- are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/group-` file contains a backup list of all the valid groups defined in the system.

### **Rationale:**

It is critical to ensure that the `/etc/group-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### **Audit:**

Run the following command to verify `/etc/group-` is mode 644 or more restrictive, `Uid` is 0/root and `Gid` is 0/root:

```
# stat -Lc "%n %a %u/%U %g/%G" /etc/group-
/etc/group- 644 0/root 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:**

`/etc/group-` 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               | <p><b>3.3 Configure Data Access Control Lists</b><br/> Configure data access control lists based on a 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><br/> 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       |

## *6.1.5 Ensure permissions on /etc/shadow are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/shadow` file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

### **Rationale:**

If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert the user accounts.

### **Audit:**

Run the following command to verify `/etc/shadow` is mode 640 or more restrictive, `Uid` is 0/root and `Gid` is 0/root:

```
# stat -Lc "%n %a %u/%U %g/%G" /etc/shadow
```

### **Example:**

```
/etc/shadow 640 0/root 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:**

`/etc/shadow` 640 0/root 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><br>Configure data access control lists based on a 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><br>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       |

## *6.1.6 Ensure permissions on /etc/shadow- are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/shadow-` file is used to store backup information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

### **Rationale:**

It is critical to ensure that the `/etc/shadow-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### **Audit:**

Run the following command to verify `/etc/shadow-` is mode 640 or more restrictive, `Uid is 0/root and Gid is 0/root`:

```
# stat -Lc "%n %a %u/%U %g/%G" /etc/shadow-
```

### **Example:**

```
/etc/shadow 640 0/root 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:**

`/etc/shadow- 640 0/root 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><br/> Configure data access control lists based on a 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><br/> 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       |

## *6.1.7 Ensure permissions on /etc/gshadow are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/gshadow` file is used to store the information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

### **Rationale:**

If attackers can gain read access to the `/etc/gshadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/gshadow` file (such as group administrators) could also be useful to subvert the group.

### **Audit:**

Run the following command to verify `/etc/gshadow` is mode 640 or more restrictive, `Uid` is 0/root and `Gid` is 0/root:

```
# stat -Lc "%n %a %u/%U %g/%G" /etc/gshadow
```

### **Example:**

```
/etc/gshadow 640 0/root 42/gshadow
```

### **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:**

`/etc/gshadow 640 0/root 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><br>Configure data access control lists based on a 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><br>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       |

## *6.1.8 Ensure permissions on /etc/gshadow- are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/gshadow-` file is used to store backup information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

### **Rationale:**

It is critical to ensure that the `/etc/gshadow-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### **Audit:**

Run the following command to verify `/etc/gshadow-` is mode 640 or more restrictive, **Uid is 0/root and Gid is 0/root**:

```
# stat -Lc "%n %a %u/%U %g/%G" /etc/gshadow-
```

### **Example:**

```
/etc/gshadow- 640 0/root 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:**

`/etc/gshadow-` 640 0/root 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><br/> Configure data access control lists based on a 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><br/> 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       |

## *6.1.9 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 "%n %a %u/%U %g/%G" /etc/shells
/etc/shells 644 0/root 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
```

### **References:**

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

### **Additional Information:**

/etc/shells 644 0/root 0/root

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <p><b>3.3 Configure Data Access Control Lists</b><br/> Configure data access control lists based on a 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><br/> 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       |

## *6.1.10 Ensure permissions on /etc/opasswd are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

/etc/security/opasswd **and it's 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 %a %u/%U %g/%G"  
/etc/security/opasswd  
  
/etc/security/opasswd 600 0/root 0/root  
-OR-  
Nothing is returned  
# [ -e "/etc/security/opasswd.old" ] && stat -Lc "%n %a %u/%U %g/%G"  
/etc/security/opasswd.old  
  
/etc/security/opasswd.old 600 0/root 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
```

## References:

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

## Additional Information:

/etc/security/opasswd 600 0/root 0/root

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>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       |

## *6.1.11 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_smash='01000'
    a_path=(); a_arr=(); a_file=(); a_dir=() # Initialize arrays
    a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path "*/containerd/*" -a !
    -path "*/kubelet/pods/*" -a ! -path "/sys/kernel/security/apparmor/*" -a ! -path
    "/snap/*" -a ! -path "/sys/fs/cgroup/memory/*")
    while read -r l_bfs; do
        a_path+=(-a ! -path "$l_bfs/*")
    done < <(findmnt -Dkerno fstype,target | awk '$1 ~ /(^s*(nfs|proc|smb)/ {print
$2}')
    # Populate array with files that will possibly fail one of the audits
    while IFS= read -r -d $'\0' l_file; do
        [ -e "$l_file" ] && a_arr+=("$(stat -Lc '%n%#a' "$l_file")")
    done < <(find / \($a_path[@]\) \) \(-type f -o -type d \) -perm -0002 -print0
2>/dev/null)
    while IFS="^" read -r l_fname l_mode; do # Test files in the array
        [ -f "$l_fname" ] && a_file+=("$l_fname") # Add WR files
        if [ -d "$l_fname" ]; then # Add directories w/o sticky bit
            [ ! $(( $l_mode & $l_smash )) -gt 0 ] && a_dir+=("$l_fname")
        fi
    done < <(printf '%s\n' "${a_arr[@]}")
    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 *\n:$l_output"
        else
            echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit failure *\n:$l_output2"
            [ -n "$l_output" ] && echo -e "- * Correctly configured *\n:$l_output"
        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_smash='01000'
    a_path=(); a_arr=() # Initialize array
    a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path "*/containerd/*" -a !
-pPath "*/kubelet/pods/*" -a ! -path "/sys/kernel/security/apparmor/*" -a ! -path
"/snap/*" -a ! -path "/sys/fs/cgroup/memory/*")
    while read -r l_bfs; do
        a_path+=(-a ! -path "$l_bfs"/*)
    done < <(findmnt -Dkerno fstype,target | awk '$1 ~ /^\s*(nfs|proc|smb)/ {print
$2}')
    # Populate array with files
    while IFS= read -r -d $'\0' l_file; do
        [ -e "$l_file" ] && a_arr+=("$(stat -Lc '%n%#a' "$l_file")")
    done < <(find / \( "${a_path[@]}" \) \ \( -type f -o -type d \) -perm -0002 -print0
2>/dev/null)
    while IFS="^" read -r l_fname l_mode; do # Test files in the array
        if [ -f "$l_fname" ]; then # Remove excess permissions from WW files
            echo -e "- File: \"$l_fname\" is mode: \"$l_mode\"\n - removing write
permission on \"$l_fname\" from \"other\""
            chmod o-w "$l_fname"
        fi
        if [ -d "$l_fname" ]; then
            if [ ! $(( l_mode & l_smash )) -gt 0 ]; then # Add sticky bit
                echo -e "- Directory: \"$l_fname\" is mode: \"$l_mode\" and doesn't have
the sticky bit set\n - Adding the sticky bit"
                chmod a+t "$l_fname"
            fi
        fi
    done < <(printf '%s\n' "${a_arr[@]}")
    unset a_path; unset a_arr # Remove array
}
```

## 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><br/> Configure data access control lists based on a 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><br/> 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 |

### *6.1.12 Ensure no unowned or ungroupped files or directories 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_path=(); a_arr=(); a_nouser=(); a_nogroup=() # Initialize arrays
    a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path "*/containerd/*" -a !
-pwd "*/kubelet/pods/*")
    while read -r l_bfs; do
        a_path+=(-a ! -path "$l_bfs"/*)
    done <<(findmnt -Dkerno fstype,target | awk '$1 ~ /^\s*(nfs|proc|smb)/ {print
$2}')
    while IFS= read -r -d $'\0' l_file; do
        [ -e "$l_file" ] && a_arr+=("$(stat -Lc '%n^%U^%G' "$l_file")") && echo "Adding:
$l_file"
        done <<(find / \( "${a_path[@]}" \) \(\ -type f -o -type d \) \(\ -nouser -o -
nogroup \) -print0 2> /dev/null)
        while IFS="^" read -r l_fname l_user l_group; do # Test files in the array
            [ "$l_user" = "UNKNOWN" ] && a_nouser+=("$l_fname")
            [ "$l_group" = "UNKNOWN" ] && a_nogroup+=("$l_fname")
        done <<< "$printf '%s\n' \"${a_arr[@]}\""
        if ! (( ${#a_nouser[@]} > 0 )); then
            l_output="$l_output\n - No unowned files or directories 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 ungrouped files or directories 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$1_output\n"
        else
            echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit failure *
:l$1_output2"
            [ -n "$l_output" ] && echo -e "\n- * Correctly configured * :\n$1_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><br>Configure data access control lists based on a 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><br>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       |

### *6.1.13 Ensure SUID and SGID files are reviewed (Manual)*

#### **Profile Applicability:**

- Level 1 - Workstation
- Level 1 - Server

#### **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_arr=(); a_suid=(); a_sgids=() # initialize arrays
    # Populate array with files that will possibly fail one of the audits
    while read -r l_mpname; do
        while IFS= read -r -d $'\0' l_file; do
            [ -e "$l_file" ] && a_arr+=("$(stat -Lc '%n^%#a' \"$l_file\")")
        done <<<(find "$l_mpname" -xdev -not -path "/run/user/*" -type f \(-perm -2000 -o -perm -4000 \) -print0)
        done <<<"$(findmnt -Derno target)"
        # Test files in the array
        while IFS="^" read -r l_fname l_mode; do
            if [ -f "$l_fname" ]; then
                l_suid_mask="04000"; l_sgids_mask="02000"
                [ $(( $l_mode & $l_suid_mask )) -gt 0 ] && a_suid+=("$l_fname")
                [ $(( $l_mode & $l_sgids_mask )) -gt 0 ] && a_sgids+=("$l_fname")
            fi
        done <<<"$(printf '%s\n' "${a_arr[@]}")"
        if ! (( ${#a_suid[@]} > 0 )); then
            l_output="$l_output\n - There are no 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><br>Configure data access control lists based on a 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><br>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       |

## *6.1.14 Ensure system command files are group-owned by root (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must have system commands group-owned by root.

### **Rationale:**

If the Ubuntu operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to Ubuntu operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### **Audit:**

Verify the system commands contained in the following directories are group-owned by root:

```
/bin  
/sbin  
/usr/bin  
/usr/sbin  
/usr/local/bin  
/usr/local/sbin
```

Run the check with the following command:

```
# find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -group root -type f -exec stat -c "%n %G" '{}' \;
```

If any system commands are returned that are not Set Group ID up on execution (SGID) files and owned by a privileged account, this is a finding.

### **Remediation:**

Configure the system commands to be protected from unauthorized access. Run the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -group root -type f ! -perm /2000 -exec chgrp root '{}' \;
```

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238378

Rule ID: SV-238378r654309\_rule

STIG ID: UBTU-20-010458

Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

## *6.1.15 Ensure system command files are owned by root (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must have system commands owned by root.

### **Rationale:**

If the Ubuntu operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to Ubuntu operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### **Audit:**

Verify the system commands contained in the following directories are owned by root:

```
/bin  
/sbin  
/usr/bin  
/usr/sbin  
/usr/local/bin  
/usr/local/sbin
```

Use the following command for the check:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -user  
root -type f -exec stat -c "%n %U" '{}' \;
```

If any system commands are returned, this is a finding.

### **Remediation:**

Configure the system commands and their respective parent directories to be protected from unauthorized access. Run the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -user  
root -type f -exec chown root '{}' \;
```

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238377

Rule ID: SV-238377r654306\_rule

STIG ID: UBTU-20-010457

Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

## *6.1.16 Ensure directories that contain system commands set to 0755 or more restrictive (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must have directories that contain system commands set to a mode of 0755 or less permissive.

### **Rationale:**

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user has in order to make access decisions regarding the deletion of audit tools.

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

### **Audit:**

Verify the system commands directories have mode 0755 or less permissive:

```
/bin  
/sbin  
/usr/bin  
/usr/sbin  
/usr/local/bin  
/usr/local/sbin
```

Check that the system command directories have mode 0755 or less permissive with the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm  
/022 -type d -exec stat -c "%n %a" '{}' \\;
```

If any directories are found to be group-writable or world-writable, this is a finding.

## **Remediation:**

Configure the system commands directories to be protected from unauthorized access.  
Run the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm /022 -type d -exec chmod -R 755 '{}' \\;
```

## **References:**

1. NIST SP 800-53 Revision 4 :: AU-9

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238344  
Rule ID: SV-238344r654207\_rule  
STIG ID: UBTU-20-010423  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

## *6.1.17 Ensure system library directories are group-owned by root (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system library directories must be group-owned by root.

### **Rationale:**

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### **Audit:**

Verify the system-wide library directories "/lib", "/lib64", and "/usr/lib" are group-owned by root with the following command:

```
# find /lib /usr/lib /lib64 ! -group root -type d -exec stat -c "%n %G" '{}' ';' \;
```

If any system-wide shared library directory is returned, this is a finding.

### **Remediation:**

Configure the system library directories to be protected from unauthorized access. Run the following command:

```
# find /lib /usr/lib /lib64 ! -group root -type d -exec chgrp root '{}' ';' \;
```

### **References:**

1. NIST SP 800-53 Revision 5 :: CM-5 (6)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238352

Rule ID: SV-238352r654231\_rule

STIG ID: UBTU-20-010431

Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

## *6.1.18 Ensure system library files are group-owned by root (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system operating system library files must be group-owned by root.

### **Rationale:**

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### **Audit:**

Verify the system-wide library files contained in the directories "/lib", "/lib64", and "/usr/lib" are group-owned by root with the following command:

```
# find /lib /usr/lib /lib64 ! -group root -type f -exec stat -c "%n %G" '{}' \;
```

If any system-wide shared library file is returned, this is a finding.

### **Remediation:**

Configure the system library files to be protected from unauthorized access. Run the following command:

```
# find /lib /usr/lib /lib64 ! -group root -type f -exec chgrp root '{}' \;
```

### **References:**

1. NIST SP 800-53 Revision 5 :: CM-5 (6)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238351  
Rule ID: SV-238351r654228\_rule  
STIG ID: UBTU-20-010430  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

## *6.1.19 Ensure system library directories are owned by root (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system library directories must be owned by root.

### **Rationale:**

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### **Audit:**

Verify the system-wide shared library directories "/lib", "/lib64", and "/usr/lib" are owned by root with the following command:

```
# find /lib /usr/lib /lib64 ! -user root -type d -exec stat -c "%n %U" '{}' ';'
```

If any system-wide library directory is returned, this is a finding.

### **Remediation:**

Configure the library files and their respective parent directories to be protected from unauthorized access. Run the following command:

```
# find /lib /usr/lib /lib64 ! -user root -type d -exec chown root '{}' ';'
```

### **References:**

1. NIST SP 800-53 Revision 5 :: CM-5 (6)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238350

Rule ID: SV-238350r654225\_rule

STIG ID: UBTU-20-010429

Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

## *6.1.20 Ensure directories that contain system commands are owned by root (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must have directories that contain system commands owned by root.

### **Rationale:**

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user has in order to make access decisions regarding the deletion of audit tools.

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

### **Audit:**

Verify the system commands directories are owned by root:

```
/bin  
/sbin  
/usr/bin  
/usr/sbin  
/usr/local/bin  
/usr/local/sbin
```

Use the following command for the check:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -user  
root -type d -exec stat -c "%n %U" '{}' \;
```

If any system commands directories are returned, this is a finding.

## **Remediation:**

Configure the system commands directories to be protected from unauthorized access.  
Run the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -user root -type d -exec chown root '{}' \;
```

## **References:**

1. NIST SP 800-53 Revision 4 :: AU-9

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238345  
Rule ID: SV-238345r654210\_rule  
STIG ID: UBTU-20-010424  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

## 6.1.21 Ensure system library files are owned by root (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system operating system library files must be owned by root.

### Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### Audit:

Verify the system-wide shared library files contained in the directories "/lib", "/lib64", and "/usr/lib" are owned by root with the following command:

```
# find /lib /usr/lib /lib64 ! -user root -type f -exec stat -c "%n %U" '{}' \;
```

If any system-wide library file is returned, this is a finding.

### Remediation:

Configure the system library files to be protected from unauthorized access. Run the following command:

```
# find /lib /usr/lib /lib64 ! -user root -type f -exec chown root '{}' \;
```

### References:

1. NIST SP 800-53 Revision 5 :: CM-5 (6)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023  
Vul ID: V-238349  
Rule ID: SV-238349r654222\_rule  
STIG ID: UBTU-20-010428  
Severity: CAT II

## **CIS Controls:**

| <b>Controls Version</b> | <b>Control</b>                                                                                                                                                                                                                                                                                                                                                                                                 | <b>IG 1</b> | <b>IG 2</b> | <b>IG 3</b> |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-------------|
| v8                      | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●           | ●           | ●           |

## *6.1.22 Ensure directories that contain system commands are group-owned by root (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must have directories that contain system commands group-owned by root.

### **Rationale:**

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user has in order to make access decisions regarding the deletion of audit tools.

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

### **Audit:**

Check Text: Verify the system commands directories are group-owned by root:

```
/bin  
/sbin  
/usr/bin  
/usr/sbin  
/usr/local/bin  
/usr/local/sbin
```

Run the check with the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -group  
root -type d -exec stat -c "%n %G" '{}' \;
```

If any system commands directories are returned that are not Set Group ID up on execution (SGID) files and owned by a privileged account, this is a finding.

## **Remediation:**

Configure the system commands directories to be protected from unauthorized access.  
Run the following command:

```
# find /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -group root -type d -exec chgrp root '{}' \;
```

## **References:**

1. NIST SP 800-53 Revision 4 :: AU-9

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023  
Vul ID: V-238346  
Rule ID: SV-238346r654213\_rule  
STIG ID: UBTU-20-010425  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

## *6.1.23 Ensure system library directories are 0755 or more restrictive (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system library directories must have mode 0755 or less permissive.

### **Rationale:**

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### **Audit:**

Verify the system-wide shared library directories "/lib", "/lib64", and "/usr/lib" have mode 0755 or less permissive with the following command:

```
# find /lib /lib64 /usr/lib -perm /022 -type d -exec stat -c "%n %a" '{}' \;
```

If any of the aforementioned directories are found to be group-writable or world-writable, this is a finding.

### **Remediation:**

Configure the shared library directories to be protected from unauthorized access. Run the following command:

```
# find /lib /lib64 /usr/lib -perm /022 -type d -exec chmod 755 '{}' \;
```

### **References:**

1. NIST SP 800-53 Revision 5 :: CM-5 (6)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238348

Rule ID: SV-238348r654219\_rule

STIG ID: UBTU-20-010427

Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

## *6.1.24 Ensure system library files are 0755 or more restrictive (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system library files must have mode 0755 or less permissive.

### **Rationale:**

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### **Audit:**

Verify the system-wide shared library files contained in the directories "/lib", "/lib64", and "/usr/lib" have mode 0755 or less permissive with the following command:

```
# find /lib /lib64 /usr/lib -perm /022 -type f -exec stat -c "%n %a" '{}' \;
/usr/lib64/pkcs11-spy.so
```

If any files are found to be group-writable or world-writable, this is a finding.

### **Remediation:**

Configure the library files to be protected from unauthorized access. Run the following command:

```
# find /lib /lib64 /usr/lib -perm /022 -type f -exec chmod 755 '{}' \;
```

### **References:**

1. NIST SP 800-53 Revision 5 :: CM-5 (6)

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 July 2023

Vul ID: V-238347  
Rule ID: SV-238347r654216\_rule  
STIG ID: UBTU-20-010426  
Severity: CAT II

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ●    | ●    | ●    |

## 6.2 Local User and Group Settings

This section provides guidance on securing aspects of the local users and groups.

**Note:** The recommendations in this section check local users and groups. Any users or groups from other sources such as LDAP will not be audited. In a domain environment similar checks should be performed against domain users and groups.

DRAFT

## *6.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Local accounts can use shadowed passwords. With shadowed passwords, the passwords are saved in shadow password file, `/etc/shadow`, encrypted by a salted one-way hash. Accounts with a shadowed password have an `x` in the second field in `/etc/passwd`.

### **Rationale:**

The `/etc/passwd` file also contains information like user ID's and group ID's that are used by many system programs. Therefore, the `/etc/passwd` file must remain world readable. In spite of encoding the password with a randomly-generated one-way hash function, an attacker could still break the system if they got access to the `/etc/passwd` file. This can be mitigated by using shadowed passwords, thus moving the passwords in the `/etc/passwd` file to `/etc/shadow`. The `/etc/shadow` file is set so only root will be able to read and write. This helps mitigate the risk of an attacker gaining access to the encoded passwords with which to perform a dictionary attack.

### **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 $1 " is not set to shadowed passwords "}'  
/etc/passwd
```

### **Remediation:**

Run the following command to set accounts to use shadowed passwords:

```
# sed -e 's/^\\([a-zA-Z0-9_]*\\):[^:]*/\\1:x:/' -i /etc/passwd
```

Investigate to determine if the account is logged in and what it is being used for, to determine if it needs to be forced off.

## 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><br>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><br>Encrypt or hash with a salt all authentication credentials when stored.                                                                                                                                                                                                                                                                                                                                    |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1003, T1003.008            | TA0003  | M1027       |

## *6.2.2 Ensure /etc/shadow password fields are not empty (Automated)*

### **Profile Applicability:**

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

### **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
2. NIST SP 800-53 :: CM-6 b

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-251503  
Rule ID: SV-251503r808506\_rule  
STIG ID: UBTU-20-010462  
Severity: CAT I

## **CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>5.2 Use Unique Passwords</b><br>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><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    | ●    | ●    | ●    |

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

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078, T1078.001, T1078.003 | TA0003  | M1027       |

### *6.2.3 Ensure all groups in /etc/passwd exist in /etc/group (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Over time, system administration errors and changes can lead to groups being defined in `/etc/passwd` but not in `/etc/group`.

#### **Rationale:**

Groups defined in the `/etc/passwd` file but not in the `/etc/group` file pose a threat to system security since group permissions are not properly managed.

#### **Audit:**

Run the following script and verify no results are returned:

```
#!/bin/bash

for i in $(cut -s -d: -f4 /etc/passwd | sort -u); do
    grep -q -P "^.+?:[^:]*:$i:" /etc/group
    if [ $? -ne 0 ]; then
        echo "Group $i is referenced by /etc/passwd but does not exist in
/etc/group"
    fi
done
```

#### **Remediation:**

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

#### **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 |
|-----------------------------|---------|-------------|
| T1222, T1222.002            | TA0003  | M1027       |

## 6.2.4 Ensure shadow group is empty (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The shadow group allows system programs which require access the ability to read the /etc/shadow file. No users should be assigned to the shadow group.

### Rationale:

Any users assigned to the shadow group would be granted read access to the /etc/shadow file. If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert additional user accounts.

### Audit:

Run the following commands and verify no results are returned:

```
# awk -F: '$1=="shadow" {print $NF}' /etc/group
# awk -F: -v GID=$(awk -F: '$1=="shadow" {print $3}' /etc/group)"
'($4==GID) {print $1}' /etc/passwd
```

### Remediation:

Run the following command to remove all users from the shadow group

```
# sed -ri 's/^(shadow:[^:]*)*:[^:]*(:[^:]*)*([^\:]+$)/\1/' /etc/group
```

Change the primary group of any users with shadow as their primary group.

```
# usermod -g <primary group> <user>
```

### 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><br/> Configure data access control lists based on a 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><br/> 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       |

## 6.2.5 Ensure no duplicate UIDs exist (Automated)

### Profile Applicability:

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

### Description:

Although the `useradd` program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the `/etc/passwd` file and change the UID field.

### Rationale:

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

### Audit:

Run the following script and verify no results are returned:

```
#!/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
2. NIST SP 800-53 :: IA-2
3. NIST SP 800-53 :: IA-8

## **Additional Information:**

Canonical Ubuntu 20.04 LTS Security Technical Implementation Guide  
Version 1, Release: 9 Benchmark Date: 26 Jul 2023

Vul ID: V-238205  
Rule ID: SV-238205r653790\_rule  
STIG ID: UBTU-20-010010  
Severity: CAT II

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

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1078, T1078.001,<br>T1078.003     | TA0005         | M1027              |

## 6.2.6 Ensure no duplicate GIDs exist (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Although the `groupadd` program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the `/etc/group` file and change the GID field.

### Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

### Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -d: -f3 /etc/group | sort | uniq -d | while read x ; do
    echo "Duplicate GID ($x) in /etc/group"
done
```

### Remediation:

Based on the results of the audit script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

### 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:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078, T1078.001, T1078.003 | TA0005  | M1027       |

## 6.2.7 Ensure no duplicate user names exist (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Although the `useradd` program will not let you create a duplicate user name, it is possible for an administrator to manually edit the `/etc/passwd` file and change the user name.

### Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in `/etc/passwd`. For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.

### Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -d: -f1 /etc/passwd | sort | uniq -d | while read -r x; do
    echo "Duplicate login name $x in /etc/passwd"
done
```

### Remediation:

Based on the results of the audit script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

### 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 | TA0004  | M1027       |

## 6.2.8 Ensure no duplicate group names exist (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Although the `groupadd` program will not let you create a duplicate group name, it is possible for an administrator to manually edit the `/etc/group` file and change the group name.

### Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in `/etc/group`. Effectively, the GID is shared, which is a security problem.

### Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -d: -f1 /etc/group | sort | uniq -d | while read -r x; do
    echo "Duplicate group name $x in /etc/group"
done
```

### Remediation:

Based on the results of the audit script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

### 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 | TA0004  | M1027       |

## 6.2.9 Ensure root PATH Integrity (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `root` user can execute any command on the system and could be fooled into executing programs unintentionally if the `PATH` is not set correctly.

### Rationale:

Including the current working directory (.) or other writable directory in `root`'s executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as `root` to execute a Trojan horse program.

### Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

RPCV=$(sudo -Hiu root env | grep '^PATH' | cut -d= -f2)
echo "$RPCV" | grep -q ":" && echo "root's path contains a empty directory (:)"
echo "$RPCV" | grep -q ":"$" && echo "root's path contains a trailing (:)"
for x in $(echo "$RPCV" | tr ":" " "); do
    if [ -d "$x" ]; then
        ls -ldH "$x" | awk '$9 == "." {print "PATH contains current working
directory (.)"}
        $3 != "root" {print $9, "is not owned by root"}
        substr($1,6,1) != "-" {print $9, "is group writable"}
        substr($1,9,1) != "-" {print $9, "is world writable"}'
    else
        echo "$x is not a directory"
    fi
done
```

### Remediation:

Correct or justify any items discovered in the Audit step.

### 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       |

DRAFT

## 6.2.10 Ensure root is the only UID 0 account (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Any account with UID 0 has superuser privileges on the system.

### Rationale:

This access must be limited to only the default `root` account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 5.6 Ensure access to the `su` command is restricted.

### Audit:

Run the following command and verify that only "root" is returned:

```
# awk -F: '($3 == 0) { print $1 }' /etc/passwd
root
```

### Remediation:

Remove any users other than `root` with UID 0 or assign them a new UID if appropriate.

### 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       |

### *6.2.11 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 "$l_output2" ]; then # If l_output2 is empty, we pass
        echo -e "\n- Audit Result:\n ** PASS **\n - * Correctly configured * :$l_output"
    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"
    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\" 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
}
```

## **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><br/> Configure data access control lists based on a 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><br/> 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       |

## *6.2.12 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 last 500 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 have permissions of 600 or more restrictive.

```

#!/usr/bin/env bash

{
    l_output="" l_output2="" l_output3="" l_output4=""
    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 ;;
                        .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"
echo -e "$l_output4"
if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass
    echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured * :\n\$l_output\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 * :\n\$l_output\n"
fi
}

```

DRAFT

### **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[0]}" # 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               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a 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><br>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, T1222.001, 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 overlayfs kernel module is not available (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.7                      | Ensure squashfs kernel module is not available (Automated)                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.8                      | Ensure udf kernel module is not available (Automated)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.9                      | Ensure usb-storage kernel module is not available (Automated)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.10                     | Ensure data-at-rest encryption is enabled (Manual)                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.11                     | Ensure data-at-rest employs cryptographic mechanisms to prevent unauthorized modification (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.12                     | Ensure sticky bit is set on all world-writable directories (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2                        | <b>Configure Filesystem Partitions</b>                                                             |                          |                          |

| CIS Benchmark Recommendation |                                                            | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                            | Yes                      | No                       |
| <b>1.1.2.1</b>               | <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"/> |
| <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"/> |

| CIS Benchmark Recommendation |                                                                                  | Set Correctly            |                          |
|------------------------------|----------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                  | Yes                      | No                       |
| 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"/> |
| <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>Configure Software and Patch Management</b>                                   |                          |                          |
| 1.2.1                        | Ensure updates, patches, and additional security software are installed (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                  | Set Correctly            |                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                  | Yes                      | No                       |
| 1.2.2                        | Ensure package manager repositories are configured (Manual)                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.3                        | Ensure GPG keys are configured (Manual)                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.4                        | Ensure apt is configured to prevent installation without verification of a recognized and approved digital signature (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.5                        | Ensure the Advance Package Tool removes all software components after updated versions have been installed (Automated)           | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.3</b>                   | <b>Secure Boot Settings</b>                                                                                                      |                          |                          |
| 1.3.1                        | Ensure bootloader password is set (Automated)                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.2                        | Ensure permissions on bootloader config are configured (Automated)                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.3                        | Ensure authentication required for single user mode (Automated)                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.4</b>                   | <b>Additional Process Hardening</b>                                                                                              |                          |                          |
| 1.4.1                        | Ensure XD/NX support is enabled (Manual)                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.2                        | Ensure address space layout randomization (ASLR) is enabled (Automated)                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.3                        | Ensure ptrace_scope is restricted (Automated)                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.4                        | Ensure prelink is not installed (Automated)                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5                        | Ensure maxlogins is 10 or less (Automated)                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.6                        | Ensure Automatic Error Reporting is not enabled (Automated)                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.7                        | Ensure kdump service is not enabled (Automated)                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.8                        | Ensure core dumps are restricted (Automated)                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                          | Set Correctly            |                          |
|------------------------------|--------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                          | Yes                      | No                       |
| 1.4.9                        | Ensure the Ctrl-Alt-Delete key sequence is disabled (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.10                       | Ensure dmesg_restrict is enabled (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.5</b>                   | <b>Mandatory Access Control</b>                                          |                          |                          |
| <b>1.5.1</b>                 | <b>Configure AppArmor</b>                                                |                          |                          |
| 1.5.1.1                      | Ensure AppArmor is installed (Automated)                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.2                      | Ensure AppArmor is enabled in the bootloader configuration (Automated)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.3                      | Ensure AppArmor is installed, enabled, and active (Automated)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.4                      | Ensure all AppArmor Profiles are in enforce or complain mode (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.5                      | Ensure all AppArmor Profiles are enforcing (Automated)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.6</b>                   | <b>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"/> |
| 1.6.3                        | Ensure remote login warning banner is configured properly (Automated)    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.4                        | Ensure permissions on /etc/motd are configured (Automated)               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.5                        | Ensure permissions on /etc/issue are configured (Automated)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.6                        | Ensure permissions on /etc/issue.net are configured (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                       | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                       | Yes                      | No                       |
| 1.7                          | <b>GNOME Display Manager</b>                                                                          |                          |                          |
| 1.7.1                        | Ensure GNOME Display Manager 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 user's session lock is enabled (Automated)                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.8                        | Ensure GDM disabling automatic mounting of removable media is not overridden (Automated)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.9                        | Ensure GDM autorun-never is enabled (Automated)                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.10                       | Ensure GDM autorun-never is not overridden (Automated)                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.11                       | Ensure XDCMP is not enabled (Automated)                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.12                       | Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.13                       | Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled (Automated)                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8                          | <b>Additional Software</b>                                                                            |                          |                          |
| 1.8.1                        | Ensure vlock is installed (Automated)                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                               | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                               | Yes                      | No                       |
| 1.8.2                        | Ensure Endpoint Security for Linux Threat Prevention is installed (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.9</b>                   | <b>Federal Information Processing Standards (FIPS) Cryptographic Modules</b>  |                          |                          |
| <b>2</b>                     | <b>Services</b>                                                               |                          |                          |
| <b>2.1</b>                   | <b>Configure Time Synchronization</b>                                         |                          |                          |
| <b>2.1.1</b>                 | <b>Ensure time synchronization is in use</b>                                  |                          |                          |
| 2.1.1.1                      | Ensure a single time synchronization daemon is in use (Automated)             | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.1.2</b>                 | <b>Configure chrony</b>                                                       |                          |                          |
| 2.1.2.1                      | Ensure chrony is configured with authorized timeserver (Manual)               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.2                      | Ensure chrony is running as user _chrony (Automated)                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.3                      | Ensure chrony is enabled and running (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.1.3</b>                 | <b>Configure systemd-timesyncd</b>                                            |                          |                          |
| 2.1.3.1                      | Ensure systemd-timesyncd configured with authorized timeserver (Automated)    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3.2                      | Ensure systemd-timesyncd is enabled and running (Manual)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.1.4</b>                 | <b>Configure ntp</b>                                                          |                          |                          |
| 2.1.4.1                      | Ensure ntp access control is configured (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.2                      | Ensure ntp is configured with authorized timeserver (Manual)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.3                      | Ensure ntp is running as user ntp (Automated)                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.4                      | Ensure ntp is enabled and running (Automated)                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                       | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                       | Yes                      | No                       |
| 2.1.5                        | Ensure system clocks are synchronize to the authoritative time source when the time difference is greater than one second (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.6                        | Ensure system clocks are synchronized with a time server designated for the appropriate DoD network (Automated)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7                        | Ensure system timezone is set to UTC or GMT (Automated)                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.2</b>                   | <b>Special Purpose Services</b>                                                                                                       |                          |                          |
| 2.2.1                        | Ensure X Window System is not installed (Automated)                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.2                        | Ensure Avahi Server is not installed (Automated)                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.3                        | Ensure CUPS is not installed (Automated)                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.4                        | Ensure DHCP Server is not installed (Automated)                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.5                        | Ensure LDAP server is not installed (Automated)                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.6                        | Ensure NFS is not installed (Automated)                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.7                        | Ensure DNS Server is not installed (Automated)                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.8                        | Ensure FTP Server is not installed (Automated)                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.9                        | Ensure HTTP server is not installed (Automated)                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.10                       | Ensure IMAP and POP3 server are not installed (Automated)                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.11                       | Ensure Samba is not installed (Automated)                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.12                       | Ensure HTTP Proxy Server is not installed (Automated)                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.13                       | Ensure SNMP Server is not installed (Automated)                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.14                       | Ensure NIS Server is not installed (Automated)                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                          | Set Correctly            |                          |
|------------------------------|--------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                          | Yes                      | No                       |
| 2.2.15                       | Ensure dnsmasq is not installed (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.16                       | Ensure mail transfer agent is configured for local-only mode (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.17                       | Ensure telnetd is not installed (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.18                       | Ensure rsync service is either not installed or is masked (Automated)    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.19                       | Ensure rsh-server is not installed (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.3</b>                   | <b>Service Clients</b>                                                   |                          |                          |
| 2.3.1                        | Ensure NIS Client is not installed (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.2                        | Ensure rsh client is not installed (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.3                        | Ensure talk client is not installed (Automated)                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.4                        | Ensure telnet client is not installed (Automated)                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.5                        | Ensure LDAP client is not installed (Automated)                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.6                        | Ensure RPC is not installed (Automated)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4                          | Ensure nonessential services are removed or masked (Manual)              | <input type="checkbox"/> | <input type="checkbox"/> |
| <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"/> |
| 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"/> |

| CIS Benchmark Recommendation |                                                                  | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                  | Yes                      | No                       |
| 3.2.2                        | Ensure sctp 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 tipc 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 tcp syn Cookies is enabled (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.9                        | Ensure source routed packets are not accepted (Automated)        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.10                       | Ensure suspicious packets are logged (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>3.4</b>                   | <b>Configure Host Based Firewall</b>                             |                          |                          |
| <b>3.4.1</b>                 | <b>Configure UncomplicatedFirewall</b>                           |                          |                          |
| 3.4.1.1                      | Ensure ufw is installed (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.2                      | Ensure iptables-persistent is not installed with ufw (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                              | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                              | Yes                      | No                       |
| 3.4.1.3                      | Ensure ufw service is enabled (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.4                      | Ensure ufw loopback traffic is configured (Automated)                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.5                      | Ensure ufw outbound connections are configured (Manual)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.6                      | Ensure ufw firewall rules exist for all open ports (Automated)               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.7                      | Ensure ufw default deny firewall policy (Automated)                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.8                      | Ensure UFW rate-limits impacted network interfaces (Manual)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>3.4.2</b>                 | <b>Configure nftables</b>                                                    |                          |                          |
| 3.4.2.1                      | Ensure nftables is installed (Automated)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.2                      | Ensure ufw is uninstalled or disabled with nftables (Automated)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.3                      | Ensure iptables are flushed with nftables (Manual)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.4                      | Ensure a nftables table exists (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.5                      | Ensure nftables base chains exist (Automated)                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.6                      | Ensure nftables loopback traffic is configured (Automated)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.7                      | Ensure nftables outbound and established connections are configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.8                      | Ensure nftables default deny firewall policy (Automated)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.9                      | Ensure nftables service is enabled (Automated)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.10                     | Ensure nftables rules are permanent (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>3.4.3</b>                 | <b>Configure iptables</b>                                                    |                          |                          |

| CIS Benchmark Recommendation |                                                                               | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                               | Yes                      | No                       |
| <b>3.4.3.1</b>               | <b>Configure iptables software</b>                                            |                          |                          |
| 3.4.3.1.1                    | Ensure iptables packages are installed (Automated)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.2                    | Ensure nftables is not installed with iptables (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.3                    | Ensure ufw is uninstalled or disabled with iptables (Automated)               | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>3.4.3.2</b>               | <b>Configure IPv4 iptables</b>                                                |                          |                          |
| 3.4.3.2.1                    | Ensure iptables default deny firewall policy (Automated)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.2                    | Ensure iptables loopback traffic is configured (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.3                    | Ensure iptables outbound and established connections are configured (Manual)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.4                    | Ensure iptables firewall rules exist for all open ports (Automated)           | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>3.4.3.3</b>               | <b>Configure IPv6 ip6tables</b>                                               |                          |                          |
| 3.4.3.3.1                    | Ensure ip6tables default deny firewall policy (Automated)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.2                    | Ensure ip6tables loopback traffic is configured (Automated)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.3                    | Ensure ip6tables outbound and established connections are configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.4                    | Ensure ip6tables firewall rules exist for all open ports (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4</b>                     | <b>Access, Authentication and Authorization</b>                               |                          |                          |
| <b>4.1</b>                   | <b>Configure job schedulers</b>                                               |                          |                          |
| <b>4.1.1</b>                 | <b>Configure cron</b>                                                         |                          |                          |
| 4.1.1.1                      | Ensure cron daemon is enabled and active (Automated)                          | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                             | Set Correctly            |                          |
|------------------------------|-----------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                             | Yes                      | No                       |
| 4.1.1.2                      | Ensure permissions on /etc/crontab are configured (Automated)               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3                      | Ensure permissions on /etc/cron.hourly are configured (Automated)           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4                      | Ensure permissions on /etc/cron.daily are configured (Automated)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5                      | Ensure permissions on /etc/cron.weekly are configured (Automated)           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.6                      | Ensure permissions on /etc/cron.monthly are configured (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.7                      | Ensure permissions on /etc/cron.d are configured (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.8                      | Ensure crontab is restricted to authorized users (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.1.2</b>                 | <b>Configure at</b>                                                         |                          |                          |
| 4.1.2.1                      | Ensure at is restricted to authorized users (Automated)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.2</b>                   | <b>Configure SSH Server</b>                                                 |                          |                          |
| 4.2.1                        | Ensure SSH is installed and active (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.2                        | Ensure permissions on /etc/ssh/sshd_config are configured (Automated)       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.3                        | Ensure permissions on SSH private host key files are configured (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.4                        | Ensure permissions on SSH public host key files are configured (Automated)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.5                        | Ensure SSH access is limited (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.6                        | Ensure SSH LogLevel is appropriate (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                    | Set Correctly            |                          |
|------------------------------|--------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                    | Yes                      | No                       |
| 4.2.7                        | Ensure SSH PAM is enabled (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.8                        | Ensure SSH root login is disabled (Automated)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.9                        | Ensure SSH HostbasedAuthentication is disabled (Automated)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.10                       | Ensure SSH PermitEmptyPasswords is disabled (Automated)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.11                       | Ensure SSH PermitUserEnvironment is disabled (Automated)           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.12                       | Ensure SSH IgnoreRhosts is enabled (Automated)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.13                       | Ensure SSH X11 forwarding is disabled (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.14                       | Ensure only strong Ciphers are used (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.15                       | Ensure only strong MAC algorithms are used (Automated)             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.16                       | Ensure only strong Key Exchange algorithms are used (Automated)    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.17                       | Ensure SSH AllowTcpForwarding is disabled (Automated)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.18                       | Ensure SSH warning banner is configured (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.19                       | Ensure SSH MaxAuthTries is set to 4 or less (Automated)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.20                       | Ensure SSH MaxStartups is configured (Automated)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.21                       | Ensure SSH LoginGraceTime is set to one minute or less (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.22                       | Ensure SSH MaxSessions is set to 10 or less (Automated)            | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                         | Set Correctly            |                          |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                         | Yes                      | No                       |
| 4.2.23                       | Ensure SSH Idle Timeout Interval is configured (Automated)                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.24                       | Ensure network connections associated with SSH traffic are terminated after a period of inactivity (Automated)                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.25                       | Ensure network connections associated with SSH traffic are terminated at the end of the session or 10 minutes of inactivity (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.26                       | Ensure Standard Mandatory DoD Notice and Consent Banner displayed before granting any local or remote connection to the system (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.27                       | Ensure only FIPS validated MAC algorithms are used (Automated)                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.28                       | Ensure only FIPS validated Ciphers are used (Automated)                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.29                       | Ensure only FIPS validated Key Exchange algorithms are used (Automated)                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.30                       | Ensure X11UseLocalhost is enabled (Automated)                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.3</b>                   | <b>Configure privilege escalation</b>                                                                                                   |                          |                          |
| 4.3.1                        | Ensure sudo is installed (Automated)                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.2                        | Ensure sudo commands use pty (Automated)                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.3                        | Ensure sudo log file exists (Automated)                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.4                        | Ensure only users who need access to security functions are part of sudo group (Manual)                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.5                        | Ensure users must provide password for privilege escalation (Automated)                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.6                        | Ensure re-authentication for privilege escalation is not disabled globally (Automated)                                                  | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                              | Set Correctly            |                          |
|------------------------------|----------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                              | Yes                      | No                       |
| 4.3.7                        | Ensure sudo authentication timeout is configured correctly (Automated)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.8                        | Ensure access to the su command is restricted (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.4</b>                   | <b>Configure Pluggable Authentication Modules</b>                                            |                          |                          |
| <b>4.4.1</b>                 | <b>Configure pam_pwquality module</b>                                                        |                          |                          |
| 4.4.1.1                      | Ensure new and changed passwords use pwquality (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.2                      | Ensure password creation requirements are configured (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.3                      | Ensure maximum number of same consecutive characters in a password is configured (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.4                      | Ensure the number of changed characters in a new password is configured (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.5                      | Ensure preventing the use of dictionary words for passwords is configured (Automated)        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.6                      | Ensure password includes at least one upper-case character (Automated)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.7                      | Ensure password includes at least one lower-case character (Automated)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.8                      | Ensure password includes at least one numeric character (Automated)                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.9                      | Ensure password includes at least one special character (Automated)                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.10                     | Ensure change of at least 8 characters when passwords are changed (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.11                     | Ensure password is at least 15 characters (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                | Set Correctly            |                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                | Yes                      | No                       |
| 4.4.2                        | <b>Configure pam_pwhistory module</b>                                                                          |                          |                          |
| 4.4.2.1                      | Ensure password reuse is limited (Automated)                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3                        | <b>Configure pam_faillock module</b>                                                                           |                          |                          |
| 4.4.3.1                      | Ensure lockout for failed password attempts is configured (Automated)                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3.2                      | Ensure lockout for three or more failed password attempts is configured (Automated)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.4                        | <b>Configure pam_unix module</b>                                                                               |                          |                          |
| 4.4.4.1                      | Ensure strong password hashing algorithm is configured (Automated)                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.4.2                      | Ensure pam modules do not include nullok (Automated)                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.5                        | <b>Configure System Security Services</b>                                                                      |                          |                          |
| 4.4.5.1                      | Ensure PAM prohibits the use of cached authentications after one day (Automated)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6                        | <b>Configure pam_pkcs11 module</b>                                                                             |                          |                          |
| 4.4.6.1                      | Ensure the libpam-pkcs11 package is installed (Automated)                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.2                      | Ensure the opensc-pkcs11 is installed (Automated)                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.3                      | Ensure authenticated identity is mapped to the user or group account for PKI-based authentication (Automated)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.4                      | Ensure smart card logins for multifactor authentication for local and network access (Automated)               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.5                      | Ensure certificates are validated by constructing a certification path to an accepted trust anchor (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                           | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                           | Yes                      | No                       |
| 4.4.6.6                      | Ensure Personal Identity Verification credentials are electronically verified (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.7                      | Ensure PKI local cache of revocation data (Automated)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.4.7</b>                 | <b>Configure pam_lastlog module</b>                                                       |                          |                          |
| 4.4.7.1                      | Ensure last successful account logon is displayed upon logon (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.4.8</b>                 | <b>Configure pam_faildelay</b>                                                            |                          |                          |
| 4.4.8.1                      | Ensure login delay after failed logon attempt (Automated)                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.9                        | Ensure all current passwords uses the configured hashing algorithm (Manual)               | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.5</b>                   | <b>User Accounts and Environment</b>                                                      |                          |                          |
| <b>4.5.1</b>                 | <b>Set Shadow Password Suite Parameters</b>                                               |                          |                          |
| 4.5.1.1                      | Ensure minimum days between password changes is configured (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.2                      | Ensure password expiration is 365 days or less (Automated)                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.3                      | Ensure password expiration warning days is 7 or more (Automated)                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.4                      | Ensure inactive password lock is 30 days or less (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.5                      | Ensure all users last password change date is in the past (Automated)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.6                      | Ensure ENCRYPT_METHOD is SHA512 (Automated)                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.7                      | Ensure temporary accounts expiration time of 72 hours or less (Manual)                    | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                                                 | Set Correctly            |                          |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                                                 | Yes                      | No                       |
| 4.5.1.8                      | Ensure root account is locked (Automated)                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.9                      | Ensure password expiration is 60 days or less (Automated)                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.10                     | Ensure emergency accounts are removed or disabled after 72 hours (Manual)                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.11                     | Ensure immediate change to a permanent password (Manual)                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.2                        | Ensure system accounts are secured (Automated)                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.3                        | Ensure default group for the root account is GID 0 (Automated)                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.4                        | Ensure default user umask is 027 or more restrictive (Automated)                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.5                        | Ensure default user shell timeout is configured (Automated)                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.6                        | Ensure default user umask is 077 or more restrictive (Automated)                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.7                        | Ensure nologin is not listed in /etc/shells (Automated)                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.8                        | Ensure default user shell timeout is 600 seconds or less (Automated)                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6                          | Ensure /etc/ssl/certs only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5</b>                     | <b>Logging and Auditing</b>                                                                                                                                     |                          |                          |
| <b>5.1</b>                   | <b>Configure Logging</b>                                                                                                                                        |                          |                          |
| <b>5.1.1</b>                 | <b>Configure journald</b>                                                                                                                                       |                          |                          |
| <b>5.1.1.1</b>               | <b>Ensure journald is configured to send logs to a remote log host</b>                                                                                          |                          |                          |

| CIS Benchmark Recommendation |                                                                                    | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                    | Yes                      | No                       |
| 5.1.1.1.1                    | Ensure systemd-journal-remote is installed (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.2                    | Ensure systemd-journal-remote is configured (Manual)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.3                    | Ensure systemd-journal-remote is enabled (Manual)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.4                    | Ensure journald is not configured to receive logs from a remote client (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.2                      | Ensure journald service is enabled (Automated)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.3                      | Ensure journald is configured to compress large log files (Automated)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.4                      | Ensure journald is configured to write logfiles to persistent disk (Automated)     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.5                      | Ensure journald is not configured to send logs to rsyslog (Manual)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.6                      | Ensure journald log rotation is configured per site policy (Manual)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.7                      | Ensure journald default file permissions configured (Manual)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.1.2</b>                 | <b>Configure rsyslog</b>                                                           |                          |                          |
| 5.1.2.1                      | Ensure rsyslog is installed (Automated)                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.2                      | Ensure rsyslog service is enabled (Automated)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.3                      | Ensure journald is configured to send logs to rsyslog (Manual)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.4                      | Ensure rsyslog default file permissions are configured (Automated)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.5                      | Ensure logging is configured (Manual)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.6                      | Ensure rsyslog is configured to send logs to a remote log host (Manual)            | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                   | Set Correctly            |                          |
|------------------------------|-----------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                   | Yes                      | No                       |
| 5.1.2.7                      | Ensure remote access methods are monitored (Automated)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.8                      | Ensure rsyslog is not configured to receive logs from a remote client (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.1.3</b>                 | <b>Configure logfile access</b>                                                   |                          |                          |
| 5.1.3.1                      | Ensure /var/log is owned by root (Automated)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.2                      | Ensure /var/log is group-owned by syslog (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.3                      | Ensure /var/log is mode 0755 or more restrictive (Automated)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.4                      | Ensure all logfiles have appropriate access configured (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.5                      | Ensure /var/log/syslog is owned by syslog (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.6                      | Ensure /var/log/syslog is group-owned by adm (Automated)                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.7                      | Ensure /var/log/syslog is 0640 or more restrictive (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.2</b>                   | <b>Configure System Accounting (auditd)</b>                                       |                          |                          |
| <b>5.2.1</b>                 | <b>Ensure auditing is enabled</b>                                                 |                          |                          |
| 5.2.1.1                      | Ensure auditd is installed (Automated)                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.2                      | Ensure auditd service is enabled and active (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.3                      | Ensure auditing for processes that start prior to auditd is enabled (Automated)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.4                      | Ensure audit_backlog_limit is sufficient (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.2.2</b>                 | <b>Configure Data Retention</b>                                                   |                          |                          |
| 5.2.2.1                      | Ensure audit log storage size is configured (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                                        | Set Correctly            |                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                                        | Yes                      | No                       |
| 5.2.2.2                      | Ensure audit logs are not automatically deleted (Automated)                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.3                      | Ensure system is disabled when audit logs are full (Automated)                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.4                      | Ensure crontab scrip running to offload audit events of standalone systems (Manual)                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.5                      | Ensure shut down by default upon audit failure (Automated)                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.6                      | Ensure security personnel are notified when storage volume reaches 75 percent utilization (Manual)                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.7                      | Ensure sufficient storage capacity to store at least one week worth of audit records (Manual)                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.8                      | Ensure audit event multiplexor is configured to off-load audit logs onto a different system or storage media from the system being audited (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.2.3</b>                 | <b>Configure auditd rules</b>                                                                                                                          |                          |                          |
| 5.2.3.1                      | Ensure changes to system administration scope (sudoers) is collected (Automated)                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.2                      | Ensure actions as another user are always logged (Automated)                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.3                      | Ensure events that modify the sudo log file are collected (Automated)                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.4                      | Ensure events that modify date and time information are collected (Automated)                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.5                      | Ensure events that modify the system's network environment are collected (Automated)                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.6                      | Ensure use of privileged commands are collected (Automated)                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                 | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                 | Yes                      | No                       |
| 5.2.3.7                      | Ensure unsuccessful file access attempts are collected (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.8                      | Ensure events that modify user/group information are collected (Automated)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.9                      | Ensure discretionary access control permission modification events are collected (Automated)    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.10                     | Ensure successful file system mounts are collected (Automated)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.11                     | Ensure session initiation information is collected (Automated)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.12                     | Ensure login and logout events are collected (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.13                     | Ensure file deletion events by users are collected (Automated)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.14                     | Ensure events that modify the system's Mandatory Access Controls are collected (Automated)      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.15                     | Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.16                     | Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.17                     | Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.18                     | Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.19                     | Ensure kernel module loading unloading and modification is collected (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.20                     | Ensure successful and unsuccessful uses of the su command are collected (Automated)             | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                             | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                             | Yes                      | No                       |
| 5.2.3.21                     | Ensure successful and unsuccessful uses of the chfn command are collected (Automated)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.22                     | Ensure successful and unsuccessful uses of the ssh-agent command are collected (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.23                     | Ensure successful and unsuccessful uses of the ssh-keysign command are collected (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.24                     | Ensure successful and unsuccessful attempts to use the fdisk command are recorded (Automated)               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.25                     | Ensure successful and unsuccessful uses of the sudo command are recorded (Automated)                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.26                     | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are recorded (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.27                     | Ensure successful and unsuccessful attempts to use the sudoedit command are recorded (Automated)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.28                     | Ensure successful and unsuccessful attempts to use the crontab command are recorded (Automated)             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.29                     | Ensure successful and unsuccessful attempts to use the chsh command are recorded (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.30                     | Ensure successful and unsuccessful attempts to use the chage command are recorded (Automated)               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.31                     | Ensure successful and unsuccessful attempts to use the newgrp command are recorded (Automated)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.32                     | Ensure successful and unsuccessful attempts to use the gpasswd command are recorded (Automated)             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.33                     | Ensure successful and unsuccessful attempts to use the unix_update command are recorded (Automated)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.34                     | Ensure successful and unsuccessful attempts to use the apparmor_parser command are recorded (Automated)     | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                | Yes                      | No                       |
| 5.2.3.35                     | Ensure successful and unsuccessful attempts to use the passwd command are recorded (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.36                     | Ensure the running and on disk configuration is the same (Manual)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.37                     | Ensure the audit configuration is immutable (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.2.4</b>                 | <b>Configure auditd file access</b>                                                            |                          |                          |
| 5.2.4.1                      | Ensure the audit log directory is 0750 or more restrictive (Automated)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.2                      | Ensure audit log files are mode 0640 or more restrictive (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.3                      | Ensure audit log files are mode 0600 or more restrictive (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.4                      | Ensure only authorized users own audit log files (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.5                      | Ensure only authorized groups own audit log files (Automated)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.6                      | Ensure audit configuration files are 640 or more restrictive (Automated)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.7                      | Ensure only authorized users own audit configuration files (Automated)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.8                      | Ensure only authorized groups own audit configuration files (Automated)                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.9                      | Ensure audit tools are 755 or more restrictive (Automated)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.10                     | Ensure only authorized users own audit tools (Automated)                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.11                     | Ensure only authorized groups own audit tools (Automated)                                      | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                            | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                            | Yes                      | No                       |
| <b>5.3</b>                   | <b>Filesystem Integrity Checking</b>                                                                       |                          |                          |
| 5.3.1                        | Ensure AIDE is installed (Automated)                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2                        | Ensure aide script to check file integrity is the default (Manual)                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3                        | Ensure filesystem integrity is regularly checked (Automated)                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.4                        | Ensure System Administrator are notified of changes to the baseline configuration or anomalies (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.5                        | Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)               | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6</b>                     | <b>System Maintenance</b>                                                                                  |                          |                          |
| <b>6.1</b>                   | <b>System File Permissions</b>                                                                             |                          |                          |
| 6.1.1                        | Ensure permissions on /etc/passwd are configured (Automated)                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.2                        | Ensure permissions on /etc/passwd- are configured (Automated)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.3                        | Ensure permissions on /etc/group are configured (Automated)                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.4                        | Ensure permissions on /etc/group- are configured (Automated)                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.5                        | Ensure permissions on /etc/shadow are configured (Automated)                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.6                        | Ensure permissions on /etc/shadow- are configured (Automated)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.7                        | Ensure permissions on /etc/gshadow are configured (Automated)                                              | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                             | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                             | Yes                      | No                       |
| 6.1.8                        | Ensure permissions on /etc/gshadow- are configured (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.9                        | Ensure permissions on /etc/shells are configured (Automated)                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.10                       | Ensure permissions on /etc/opasswd are configured (Automated)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.11                       | Ensure world writable files and directories are secured (Automated)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.12                       | Ensure no unowned or ungrouped files or directories exist (Automated)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.13                       | Ensure SUID and SGID files are reviewed (Manual)                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.14                       | Ensure system command files are group-owned by root (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.15                       | Ensure system command files are owned by root (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.16                       | Ensure directories that contain system commands set to 0755 or more restrictive (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.17                       | Ensure system library directories are group-owned by root (Automated)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.18                       | Ensure system library files are group-owned by root (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.19                       | Ensure system library directories are owned by root (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.20                       | Ensure directories that contain system commands are owned by root (Automated)               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.21                       | Ensure system library files are owned by root (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                     | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                     | Yes                      | No                       |
| 6.1.22                       | Ensure directories that contain system commands are group-owned by root (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.23                       | Ensure system library directories are 0755 or more restrictive (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.24                       | Ensure system library files are 0755 or more restrictive (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6.2</b>                   | <b>Local User and Group Settings</b>                                                |                          |                          |
| 6.2.1                        | Ensure accounts in /etc/passwd use shadowed passwords (Automated)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2                        | Ensure /etc/shadow password fields are not empty (Automated)                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3                        | Ensure all groups in /etc/passwd exist in /etc/group (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.4                        | Ensure shadow group is empty (Automated)                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.5                        | Ensure no duplicate UIDs exist (Automated)                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.6                        | Ensure no duplicate GIDs exist (Automated)                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.7                        | Ensure no duplicate user names exist (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.8                        | Ensure no duplicate group names exist (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.9                        | Ensure root PATH Integrity (Automated)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.10                       | Ensure root is the only UID 0 account (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.11                       | Ensure local interactive user home directories are configured (Automated)           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.12                       | 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                       |
| 1.1.1.12       | Ensure sticky bit is set on all world-writable directories              | <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"/> |
| 1.1.2.6.2      | 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          | Ensure updates, patches, and additional security software are installed | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2          | Ensure package manager repositories are configured                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.3          | Ensure GPG keys are configured                                          | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                      | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                      | Yes                      | No                       |
| 1.2.4          | Ensure apt is configured to prevent installation without verification of a recognized and approved digital signature | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.5          | Ensure the Advance Package Tool removes all software components after updated versions have been installed           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.2          | Ensure permissions on bootloader config are configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5          | Ensure maxlogins is 10 or less                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.9          | Ensure the Ctrl-Alt-Delete key sequence is disabled                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.1        | Ensure AppArmor is installed                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.2        | Ensure AppArmor is enabled in the bootloader configuration                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.4        | Ensure all AppArmor Profiles are in enforce or complain mode                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.5        | Ensure all AppArmor Profiles are enforcing                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.4          | Ensure permissions on /etc/motd are configured                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.5          | Ensure permissions on /etc/issue are configured                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.6          | Ensure permissions on /etc/issue.net are 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"/> |
| 1.7.7          | Ensure user's session lock is enabled                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.9          | Ensure GDM autorun-never is enabled                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.10         | Ensure GDM autorun-never is not overridden                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.12         | Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.13         | Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.1          | Ensure vlock is installed                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7          | Ensure system timezone is set to UTC or GMT                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.1          | Ensure X Window System is not installed                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.1          | Ensure NIS Client is not installed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.10         | Ensure suspicious packets are logged                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                      | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                      | Yes                      | No                       |
| 3.4.1.1        | Ensure ufw is installed                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.2        | Ensure iptables-persistent is not installed with ufw                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.3        | Ensure ufw service is enabled                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.4        | Ensure ufw loopback traffic is configured                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.5        | Ensure ufw outbound connections are configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.6        | Ensure ufw firewall rules exist for all open ports                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.7        | Ensure ufw default deny firewall policy                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.8        | Ensure UFW rate-limits impacted network interfaces                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.1        | Ensure nftables is installed                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.2        | Ensure ufw is uninstalled or disabled with nftables                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.3        | Ensure iptables are flushed with nftables                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.4        | Ensure a nftables table exists                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.5        | Ensure nftables base chains exist                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.6        | Ensure nftables loopback traffic is configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.7        | Ensure nftables outbound and established connections are configured  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.8        | Ensure nftables default deny firewall policy                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.9        | Ensure nftables service is enabled                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.10       | Ensure nftables rules are permanent                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.1      | Ensure iptables packages are installed                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.2      | Ensure nftables is not installed with iptables                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.3      | Ensure ufw is uninstalled or disabled with iptables                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.1      | Ensure iptables default deny firewall policy                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.2      | Ensure iptables loopback traffic is configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.3      | Ensure iptables outbound and established connections are configured  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.4      | Ensure iptables firewall rules exist for all open ports              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.1      | Ensure ip6tables default deny firewall policy                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.2      | Ensure ip6tables loopback traffic is configured                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.3      | Ensure ip6tables outbound and established connections are configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.4      | Ensure ip6tables firewall rules exist for all open ports             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                | Yes                      | No                       |
| 4.1.1.2        | Ensure permissions on /etc/crontab are configured                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3        | Ensure permissions on /etc/cron.hourly are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4        | Ensure permissions on /etc/cron.daily are configured                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5        | Ensure permissions on /etc/cron.weekly are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.6        | Ensure permissions on /etc/cron.monthly are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.7        | Ensure permissions on /etc/cron.d are configured                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.8        | Ensure crontab is restricted to authorized users                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.1        | Ensure at is restricted to authorized users                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.2          | Ensure permissions on /etc/ssh/sshd_config are configured                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.3          | Ensure permissions on SSH private host key files are configured                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.4          | Ensure permissions on SSH public host key files are configured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.5          | Ensure SSH access is limited                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.6          | Ensure SSH LogLevel is appropriate                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.8          | Ensure SSH root login is disabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.20         | Ensure SSH MaxStartups is configured                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.24         | Ensure network connections associated with SSH traffic are terminated after a period of inactivity                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.25         | Ensure network connections associated with SSH traffic are terminated at the end of the session or 10 minutes of inactivity    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.26         | Ensure Standard Mandatory DoD Notice and Consent Banner displayed before granting any local or remote connection to the system | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.30         | Ensure X11UseLocalhost is enabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.1          | Ensure sudo is installed                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.2          | Ensure sudo commands use pty                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.4          | Ensure only users who need access to security functions are part of sudo group                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.5          | Ensure users must provide password for privilege escalation                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                     | Set Correctly            |                          |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                     | Yes                      | No                       |
| 4.3.6          | Ensure re-authentication for privilege escalation is not disabled globally                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.7          | Ensure sudo authentication timeout is configured correctly                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.8          | Ensure access to the su command is restricted                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.5.1        | Ensure PAM prohibits the use of cached authentications after one day                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.7.1        | Ensure last successful account logon is displayed upon logon                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.8.1        | Ensure login delay after failed logon attempt                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.8        | Ensure root account is locked                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.10       | Ensure emergency accounts are removed or disabled after 72 hours                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.11       | Ensure immediate change to a permanent password                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.2          | Ensure system accounts are secured                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.3          | Ensure default group for the root account is GID 0                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.4          | Ensure default user umask is 027 or more restrictive                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.5          | Ensure default user shell timeout is configured                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.6          | Ensure default user umask is 077 or more restrictive                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.8          | Ensure default user shell timeout is 600 seconds or less                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure /etc/ssl/certs only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.1      | Ensure systemd-journal-remote is installed                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.2      | Ensure systemd-journal-remote is configured                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.3      | Ensure systemd-journal-remote is enabled                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.4      | Ensure journald is not configured to receive logs from a remote client                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.2        | Ensure journald service is enabled                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.3        | Ensure journald is configured to compress large log files                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.4        | Ensure journald is configured to write logfiles to persistent disk                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.5        | Ensure journald is not configured to send logs to rsyslog                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.6        | Ensure journald log rotation is configured per site policy                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                            | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                            | Yes                      | No                       |
| 5.1.1.7        | Ensure journald default file permissions configured                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.1        | Ensure rsyslog is installed                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.2        | Ensure rsyslog service is enabled                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.3        | Ensure journald is configured to send logs to rsyslog                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.4        | Ensure rsyslog default file permissions are configured                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.5        | Ensure logging is configured                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.6        | Ensure rsyslog is configured to send logs to a remote log host                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.7        | Ensure remote access methods are monitored                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.8        | Ensure rsyslog is not configured to receive logs from a remote client                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.1        | Ensure /var/log is owned by root                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.2        | Ensure /var/log is group-owned by syslog                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.3        | Ensure /var/log is mode 0755 or more restrictive                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.4        | Ensure all logfiles have appropriate access configured                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.5        | Ensure /var/log/syslog is owned by syslog                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.6        | Ensure /var/log/syslog is group-owned by adm                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.7        | Ensure /var/log/syslog is 0640 or more restrictive                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.1        | Ensure auditd is installed                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.2        | Ensure auditd service is enabled and active                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.3        | Ensure auditing for processes that start prior to auditd is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.4        | Ensure audit_backlog_limit is sufficient                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.8        | Ensure audit event multiplexor is configured to off-load audit logs onto a different system or storage media from the system being audited | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.6        | Ensure use of privileged commands are collected                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.12       | Ensure login and logout events are collected                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.13       | Ensure file deletion events by users are collected                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.15       | Ensure successful and unsuccessful attempts to use the chcon command are recorded                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.16       | Ensure successful and unsuccessful attempts to use the setfacl command are recorded                                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                 | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                 | Yes                      | No                       |
| 5.2.3.17       | Ensure successful and unsuccessful attempts to use the chacl command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.18       | Ensure successful and unsuccessful attempts to use the usermod command are recorded             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.19       | Ensure kernel module loading unloading and modification is collected                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.20       | Ensure successful and unsuccessful uses of the su command are collected                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.21       | Ensure successful and unsuccessful uses of the chfn command are collected                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.22       | Ensure successful and unsuccessful uses of the ssh-agent command are collected                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.23       | Ensure successful and unsuccessful uses of the ssh-keysign command are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.24       | Ensure successful and unsuccessful attempts to use the fdisk command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.25       | Ensure successful and unsuccessful uses of the sudo command are recorded                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.26       | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are recorded | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.27       | Ensure successful and unsuccessful attempts to use the sudoedit command are recorded            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.28       | Ensure successful and unsuccessful attempts to use the crontab command are recorded             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.29       | Ensure successful and unsuccessful attempts to use the chsh command are recorded                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.30       | Ensure successful and unsuccessful attempts to use the chage command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.31       | Ensure successful and unsuccessful attempts to use the newgrp command are recorded              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.32       | Ensure successful and unsuccessful attempts to use the gpasswd command are recorded             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.33       | Ensure successful and unsuccessful attempts to use the unix_update command are recorded         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.34       | Ensure successful and unsuccessful attempts to use the apparmor_parser command are recorded     | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                    | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                    | Yes                      | No                       |
| 5.2.3.35       | Ensure successful and unsuccessful attempts to use the passwd command are recorded | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.37       | Ensure the audit configuration is immutable                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.1        | Ensure the audit log directory is 0750 or more restrictive                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.2        | Ensure audit log files are mode 0640 or more restrictive                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.3        | Ensure audit log files are mode 0600 or more restrictive                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.4        | Ensure only authorized users own audit log files                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.5        | Ensure only authorized groups own audit log files                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.6        | Ensure audit configuration files are 640 or more restrictive                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.7        | Ensure only authorized users own audit configuration files                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.8        | Ensure only authorized groups own audit configuration files                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.9        | Ensure audit tools are 755 or more restrictive                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.10       | Ensure only authorized users own audit tools                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.11       | Ensure only authorized groups own audit tools                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2          | Ensure aide script to check file integrity is the default                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.1          | Ensure permissions on /etc/passwd are configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.2          | Ensure permissions on /etc/passwd- are configured                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.3          | Ensure permissions on /etc/group are configured                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.4          | Ensure permissions on /etc/group- are configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.5          | Ensure permissions on /etc/shadow are configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.6          | Ensure permissions on /etc/shadow- are configured                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.7          | Ensure permissions on /etc/gshadow are configured                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.8          | Ensure permissions on /etc/gshadow- are configured                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.9          | Ensure permissions on /etc/shells are configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.10         | Ensure permissions on /etc/opasswd are configured                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.11         | Ensure world writable files and directories are secured                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.12         | Ensure no unowned or ungrouped files or directories exist                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.13         | Ensure SUID and SGID files are reviewed                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.14         | Ensure system command files are group-owned by root                                | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                 | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                 | Yes                      | No                       |
| 6.1.15         | Ensure system command files are owned by root                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.16         | Ensure directories that contain system commands set to 0755 or more restrictive | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.17         | Ensure system library directories are group-owned by root                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.18         | Ensure system library files are group-owned by root                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.19         | Ensure system library directories are owned by root                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.20         | Ensure directories that contain system commands are owned by root               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.21         | Ensure system library files are owned by root                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.22         | Ensure directories that contain system commands are group-owned by root         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.23         | Ensure system library directories are 0755 or more restrictive                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.24         | Ensure system library files are 0755 or more restrictive                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.4          | Ensure shadow group is empty                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.11         | Ensure local interactive user home directories are configured                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.12         | 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 overlayfs kernel module is not available            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.7        | Ensure squashfs kernel module is not available             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.8        | Ensure udf kernel module is not available                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.9        | Ensure usb-storage kernel module is not available          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.12       | Ensure sticky bit is set on all world-writable directories | <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"/> |

| Recommendation |                                                                                                                      | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                      | Yes                      | No                       |
| 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          | Ensure updates, patches, and additional security software are installed                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2          | Ensure package manager repositories are configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.3          | Ensure GPG keys are configured                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.4          | Ensure apt is configured to prevent installation without verification of a recognized and approved digital signature | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.5          | Ensure the Advance Package Tool removes all software components after updated versions have been installed           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1          | Ensure bootloader password is set                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.2          | Ensure permissions on bootloader config are configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.3          | Ensure authentication required for single user mode                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.1          | Ensure XD/NX support is enabled                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.2          | Ensure address space layout randomization (ASLR) is enabled                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.3          | Ensure ptrace_scope is restricted                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5          | Ensure maxlogins is 10 or less                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.6          | Ensure Automatic Error Reporting is not enabled                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.7          | Ensure kdump service is not enabled                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.9          | Ensure the Ctrl-Alt-Delete key sequence is disabled                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.10         | Ensure dmesg_restrict is enabled                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.1        | Ensure AppArmor is installed                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.2        | Ensure AppArmor is enabled in the bootloader configuration                                                           | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                              | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                              | Yes                      | No                       |
| 1.5.1.4        | Ensure all AppArmor Profiles are in enforce or complain mode                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.5        | Ensure all AppArmor Profiles are enforcing                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.4          | Ensure permissions on /etc/motd are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.5          | Ensure permissions on /etc/issue are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.6          | Ensure permissions on /etc/issue.net are configured                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.1          | Ensure GNOME Display Manager 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"/> |
| 1.7.7          | Ensure user's session lock is enabled                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.9          | Ensure GDM autorun-never is enabled                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.10         | Ensure GDM autorun-never is not overridden                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.11         | Ensure XDCMP is not enabled                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.12         | Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.13         | Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.1          | Ensure vlock is installed                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.2          | Ensure Endpoint Security for Linux Threat Prevention is installed                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.1.1        | Ensure a single time synchronization daemon is in use                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.1        | Ensure chrony is configured with authorized timeserver                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.2        | Ensure chrony is running as user _chrony                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.3        | Ensure chrony is enabled and running                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3.1        | Ensure systemd-timesyncd configured with authorized timeserver                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3.2        | Ensure systemd-timesyncd is enabled and running                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.1        | Ensure ntp access control is configured                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.2        | Ensure ntp is configured with authorized timeserver                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.3        | Ensure ntp is running as user ntp                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.4        | Ensure ntp is enabled and running                                                            | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                           | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                           | Yes                      | No                       |
| 2.1.5          | Ensure system clocks are synchronize to the authoritative time source when the time difference is greater than one second | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.6          | Ensure system clocks are synchronized with a time server designated for the appropriate DoD network                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7          | Ensure system timezone is set to UTC or GMT                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.1          | Ensure X Window System is not installed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.2          | Ensure Avahi Server is not installed                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.3          | Ensure CUPS is not installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.4          | Ensure DHCP Server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.5          | Ensure LDAP server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.6          | Ensure NFS is not installed                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.7          | Ensure DNS Server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.8          | Ensure FTP Server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.9          | Ensure HTTP server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.10         | Ensure IMAP and POP3 server are not installed                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.11         | Ensure Samba is not installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.12         | Ensure HTTP Proxy Server is not installed                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.13         | Ensure SNMP Server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.14         | Ensure NIS Server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.15         | Ensure dnsmasq is not installed                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.16         | Ensure mail transfer agent is configured for local-only mode                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.17         | Ensure telnetd is not installed                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.18         | Ensure rsync service is either not installed or is masked                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.19         | Ensure rsh-server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.1          | Ensure NIS Client is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.2          | Ensure rsh client is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.3          | Ensure talk client is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.4          | Ensure telnet client is not installed                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.5          | Ensure LDAP client is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.6          | Ensure RPC is not installed                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                      | Set Correctly            |                          |
|----------------|------------------------------------------------------|--------------------------|--------------------------|
|                |                                                      | Yes                      | No                       |
| 2.4            | Ensure nonessential services are removed or masked   | <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 sctp 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 tipc 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 tcp syn Cookies is enabled                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.9          | Ensure source routed packets are not accepted        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.10         | Ensure suspicious packets are logged                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.11         | Ensure ipv6 router advertisements are not accepted   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.1        | Ensure ufw is installed                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.2        | Ensure iptables-persistent is not installed with ufw | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.3        | Ensure ufw service is enabled                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.4        | Ensure ufw loopback traffic is configured            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.5        | Ensure ufw outbound connections are configured       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.6        | Ensure ufw firewall rules exist for all open ports   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.7        | Ensure ufw default deny firewall policy              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.8        | Ensure UFW rate-limits impacted network interfaces   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.1        | Ensure nftables is installed                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.2        | Ensure ufw is uninstalled or disabled with nftables  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.3        | Ensure iptables are flushed with nftables            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.4        | Ensure a nftables table exists                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.5        | Ensure nftables base chains exist                    | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                      | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                      | Yes                      | No                       |
| 3.4.2.6        | Ensure nftables loopback traffic is configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.7        | Ensure nftables outbound and established connections are configured  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.8        | Ensure nftables default deny firewall policy                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.9        | Ensure nftables service is enabled                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.10       | Ensure nftables rules are permanent                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.1      | Ensure iptables packages are installed                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.2      | Ensure nftables is not installed with iptables                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.3      | Ensure ufw is uninstalled or disabled with iptables                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.1      | Ensure iptables default deny firewall policy                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.2      | Ensure iptables loopback traffic is configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.3      | Ensure iptables outbound and established connections are configured  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.4      | Ensure iptables firewall rules exist for all open ports              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.1      | Ensure ip6tables default deny firewall policy                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.2      | Ensure ip6tables loopback traffic is configured                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.3      | Ensure ip6tables outbound and established connections are configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.4      | Ensure ip6tables firewall rules exist for all open ports             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.2        | Ensure permissions on /etc/crontab are configured                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3        | Ensure permissions on /etc/cron.hourly are configured                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4        | Ensure permissions on /etc/cron.daily are configured                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5        | Ensure permissions on /etc/cron.weekly are configured                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.6        | Ensure permissions on /etc/cron.monthly are configured               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.7        | Ensure permissions on /etc/cron.d are configured                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.8        | Ensure crontab is restricted to authorized users                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.1        | Ensure at is restricted to authorized users                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.1          | Ensure SSH is installed and active                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.2          | Ensure permissions on /etc/ssh/sshd_config are configured            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.3          | Ensure permissions on SSH private host key files are configured      | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                | Yes                      | No                       |
| 4.2.4          | Ensure permissions on SSH public host key files are configured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.5          | Ensure SSH access is limited                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.6          | Ensure SSH LogLevel is appropriate                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.7          | Ensure SSH PAM is enabled                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.8          | Ensure SSH root login is disabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.10         | Ensure SSH PermitEmptyPasswords is disabled                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.12         | Ensure SSH IgnoreRhosts is enabled                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.13         | Ensure SSH X11 forwarding is disabled                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.14         | Ensure only strong Ciphers are used                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.15         | Ensure only strong MAC algorithms are used                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.16         | Ensure only strong Key Exchange algorithms are used                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.20         | Ensure SSH MaxStartups is configured                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.24         | Ensure network connections associated with SSH traffic are terminated after a period of inactivity                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.25         | Ensure network connections associated with SSH traffic are terminated at the end of the session or 10 minutes of inactivity    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.26         | Ensure Standard Mandatory DoD Notice and Consent Banner displayed before granting any local or remote connection to the system | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.27         | Ensure only FIPS validated MAC algorithms are used                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.28         | Ensure only FIPS validated Ciphers are used                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.29         | Ensure only FIPS validated Key Exchange algorithms are used                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.30         | Ensure X11UseLocalhost is enabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.1          | Ensure sudo is installed                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.2          | Ensure sudo commands use pty                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.3          | Ensure sudo log file exists                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.4          | Ensure only users who need access to security functions are part of sudo group                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.5          | Ensure users must provide password for privilege escalation                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                   | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                   | Yes                      | No                       |
| 4.3.6          | Ensure re-authentication for privilege escalation is not disabled globally                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.7          | Ensure sudo authentication timeout is configured correctly                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.8          | Ensure access to the su command is restricted                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.1        | Ensure new and changed passwords use pwquality                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.2        | Ensure password creation requirements are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.3        | Ensure maximum number of same consecutive characters in a password is configured                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.4        | Ensure the number of changed characters in a new password is configured                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.5        | Ensure preventing the use of dictionary words for passwords is configured                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.6        | Ensure password includes at least one upper-case character                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.7        | Ensure password includes at least one lower-case character                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.8        | Ensure password includes at least one numeric character                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.9        | Ensure password includes at least one special character                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.10       | Ensure change of at least 8 characters when passwords are changed                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.11       | Ensure password is at least 15 characters                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.2.1        | Ensure password reuse is limited                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3.1        | Ensure lockout for failed password attempts is configured                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3.2        | Ensure lockout for three or more failed password attempts is configured                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.4.1        | Ensure strong password hashing algorithm is configured                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.4.2        | Ensure pam modules do not include nullok                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.5.1        | Ensure PAM prohibits the use of cached authentications after one day                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.1        | Ensure the libpam-pkcs11 package is installed                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.2        | Ensure the opensc-pkcs11 is installed                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.3        | Ensure authenticated identity is mapped to the user or group account for PKI-based authentication | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                    | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                    | Yes                      | No                       |
| 4.4.6.4        | Ensure smart card logins for multifactor authentication for local and network access               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.5        | Ensure certificates are validated by constructing a certification path to an accepted trust anchor | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.6        | Ensure Personal Identity Verification credentials are electronically verified                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.7        | Ensure PKI local cache of revocation data                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.7.1        | Ensure last successful account logon is displayed upon logon                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.8.1        | Ensure login delay after failed logon attempt                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.9          | Ensure all current passwords uses the configured hashing algorithm                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.1        | Ensure minimum days between password changes is configured                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.2        | Ensure password expiration is 365 days or less                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.3        | Ensure password expiration warning days is 7 or more                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.4        | Ensure inactive password lock is 30 days or less                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.5        | Ensure all users last password change date is in the past                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.6        | Ensure ENCRYPT_METHOD is SHA512                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.7        | Ensure temporary accounts expiration time of 72 hours or less                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.8        | Ensure root account is locked                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.9        | Ensure password expiration is 60 days or less                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.10       | Ensure emergency accounts are removed or disabled after 72 hours                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.11       | Ensure immediate change to a permanent password                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.2          | Ensure system accounts are secured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.3          | Ensure default group for the root account is GID 0                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.4          | Ensure default user umask is 027 or more restrictive                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.5          | Ensure default user shell timeout is configured                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.6          | Ensure default user umask is 077 or more restrictive                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.8          | Ensure default user shell timeout is 600 seconds or less                                           | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                     | Set Correctly            |                          |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                     | Yes                      | No                       |
| 4.6            | Ensure /etc/ssl/certs only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.1      | Ensure systemd-journal-remote is installed                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.2      | Ensure systemd-journal-remote is configured                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.3      | Ensure systemd-journal-remote is enabled                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.4      | Ensure journald is not configured to receive logs from a remote client                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.2        | Ensure journald service is enabled                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.3        | Ensure journald is configured to compress large log files                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.4        | Ensure journald is configured to write logfiles to persistent disk                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.5        | Ensure journald is not configured to send logs to rsyslog                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.6        | Ensure journald log rotation is configured per site policy                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.7        | Ensure journald default file permissions configured                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.1        | Ensure rsyslog is installed                                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.2        | Ensure rsyslog service is enabled                                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.3        | Ensure journald is configured to send logs to rsyslog                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.4        | Ensure rsyslog default file permissions are configured                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.5        | Ensure logging is configured                                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.6        | Ensure rsyslog is configured to send logs to a remote log host                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.7        | Ensure remote access methods are monitored                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.8        | Ensure rsyslog is not configured to receive logs from a remote client                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.1        | Ensure /var/log is owned by root                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.2        | Ensure /var/log is group-owned by syslog                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.3        | Ensure /var/log is mode 0755 or more restrictive                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.4        | Ensure all logfiles have appropriate access configured                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.5        | Ensure /var/log/syslog is owned by syslog                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.6        | Ensure /var/log/syslog is group-owned by adm                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.7        | Ensure /var/log/syslog is 0640 or more restrictive                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.1        | Ensure auditd is installed                                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                            | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                            | Yes                      | No                       |
| 5.2.1.2        | Ensure auditd service is enabled and active                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.3        | Ensure auditing for processes that start prior to auditd is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.4        | Ensure audit_backlog_limit is sufficient                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.1        | Ensure audit log storage size is configured                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.2        | Ensure audit logs are not automatically deleted                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.3        | Ensure system is disabled when audit logs are full                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.4        | Ensure crontab scrip running to offload audit events of standalone systems                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.5        | Ensure shut down by default upon audit failure                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.6        | Ensure security personnel are notified when storage volume reaches 75 percent utilization                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.7        | Ensure sufficient storage capacity to store at least one week worth of audit records                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.8        | Ensure audit event multiplexor is configured to off-load audit logs onto a different system or storage media from the system being audited | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.1        | Ensure changes to system administration scope (sudoers) is collected                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.2        | Ensure actions as another user are always logged                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.3        | Ensure events that modify the sudo log file are collected                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.4        | Ensure events that modify date and time information are collected                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.5        | Ensure events that modify the system's network environment are collected                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.6        | Ensure use of privileged commands are collected                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.8        | Ensure events that modify user/group information are collected                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.9        | Ensure discretionary access control permission modification events are collected                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.10       | Ensure successful file system mounts are collected                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.11       | Ensure session initiation information is collected                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.12       | Ensure login and logout events are collected                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.13       | Ensure file deletion events by users are collected                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                 | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                 | Yes                      | No                       |
| 5.2.3.14       | Ensure events that modify the system's Mandatory Access Controls are collected                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.15       | Ensure successful and unsuccessful attempts to use the chcon command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.16       | Ensure successful and unsuccessful attempts to use the setfacl command are recorded             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.17       | Ensure successful and unsuccessful attempts to use the chacl command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.18       | Ensure successful and unsuccessful attempts to use the usermod command are recorded             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.19       | Ensure kernel module loading unloading and modification is collected                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.20       | Ensure successful and unsuccessful uses of the su command are collected                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.21       | Ensure successful and unsuccessful uses of the chfn command are collected                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.22       | Ensure successful and unsuccessful uses of the ssh-agent command are collected                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.23       | Ensure successful and unsuccessful uses of the ssh-keysign command are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.24       | Ensure successful and unsuccessful attempts to use the fdisk command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.25       | Ensure successful and unsuccessful uses of the sudo command are recorded                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.26       | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are recorded | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.27       | Ensure successful and unsuccessful attempts to use the sudoedit command are recorded            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.28       | Ensure successful and unsuccessful attempts to use the crontab command are recorded             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.29       | Ensure successful and unsuccessful attempts to use the chsh command are recorded                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.30       | Ensure successful and unsuccessful attempts to use the chage command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.31       | Ensure successful and unsuccessful attempts to use the newgrp command are recorded              | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                             | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                             | Yes                      | No                       |
| 5.2.3.32       | Ensure successful and unsuccessful attempts to use the gpasswd command are recorded         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.33       | Ensure successful and unsuccessful attempts to use the unix_update command are recorded     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.34       | Ensure successful and unsuccessful attempts to use the apparmor_parser command are recorded | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.35       | Ensure successful and unsuccessful attempts to use the passwd command are recorded          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.36       | Ensure the running and on disk configuration is the same                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.37       | Ensure the audit configuration is immutable                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.1        | Ensure the audit log directory is 0750 or more restrictive                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.2        | Ensure audit log files are mode 0640 or more restrictive                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.3        | Ensure audit log files are mode 0600 or more restrictive                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.4        | Ensure only authorized users own audit log files                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.5        | Ensure only authorized groups own audit log files                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.6        | Ensure audit configuration files are 640 or more restrictive                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.7        | Ensure only authorized users own audit configuration files                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.8        | Ensure only authorized groups own audit configuration files                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.9        | Ensure audit tools are 755 or more restrictive                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.10       | Ensure only authorized users own audit tools                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.11       | Ensure only authorized groups own audit tools                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2          | Ensure aide script to check file integrity is the default                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.1          | Ensure permissions on /etc/passwd are configured                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.2          | Ensure permissions on /etc/passwd- are configured                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.3          | Ensure permissions on /etc/group are configured                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.4          | Ensure permissions on /etc/group- are configured                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.5          | Ensure permissions on /etc/shadow are configured                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.6          | Ensure permissions on /etc/shadow- are configured                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.7          | Ensure permissions on /etc/gshadow are configured                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.8          | Ensure permissions on /etc/gshadow- are configured                                          | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                 | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                 | Yes                      | No                       |
| 6.1.9          | Ensure permissions on /etc/shells are configured                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.10         | Ensure permissions on /etc/opasswd are configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.11         | Ensure world writable files and directories are secured                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.12         | Ensure no unowned or ungrouped files or directories exist                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.13         | Ensure SUID and SGID files are reviewed                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.14         | Ensure system command files are group-owned by root                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.15         | Ensure system command files are owned by root                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.16         | Ensure directories that contain system commands set to 0755 or more restrictive | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.17         | Ensure system library directories are group-owned by root                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.18         | Ensure system library files are group-owned by root                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.19         | Ensure system library directories are owned by root                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.20         | Ensure directories that contain system commands are owned by root               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.21         | Ensure system library files are owned by root                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.22         | Ensure directories that contain system commands are group-owned by root         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.23         | Ensure system library directories are 0755 or more restrictive                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.24         | Ensure system library files are 0755 or more restrictive                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1          | Ensure accounts in /etc/passwd use shadowed passwords                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2          | Ensure /etc/shadow password fields are not empty                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.4          | Ensure shadow group is empty                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.11         | Ensure local interactive user home directories are configured                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.12         | 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 overlayfs kernel module is not available                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.7        | Ensure squashfs kernel module is not available                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.8        | Ensure udf kernel module is not available                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.9        | Ensure usb-storage kernel module is not available                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.10       | Ensure data-at-rest encryption is enabled                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.11       | Ensure data-at-rest employs cryptographic mechanisms to prevent unauthorized modification | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.12       | Ensure sticky bit is set on all world-writable directories                                | <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"/> |

| Recommendation |                                                                                                                      | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                      | Yes                      | No                       |
| 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          | Ensure updates, patches, and additional security software are installed                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2          | Ensure package manager repositories are configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.3          | Ensure GPG keys are configured                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.4          | Ensure apt is configured to prevent installation without verification of a recognized and approved digital signature | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.5          | Ensure the Advance Package Tool removes all software components after updated versions have been installed           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1          | Ensure bootloader password is set                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.2          | Ensure permissions on bootloader config are configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.3          | Ensure authentication required for single user mode                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.1          | Ensure XD/NX support is enabled                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.2          | Ensure address space layout randomization (ASLR) is enabled                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.3          | Ensure ptrace_scope is restricted                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.4          | Ensure prelink is not installed                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5          | Ensure maxlogins is 10 or less                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.6          | Ensure Automatic Error Reporting is not enabled                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.7          | Ensure kdump service is not enabled                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.9          | Ensure the Ctrl-Alt-Delete key sequence is disabled                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                              | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                              | Yes                      | No                       |
| 1.4.10         | Ensure dmesg_restrict is enabled                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.1        | Ensure AppArmor is installed                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.2        | Ensure AppArmor is enabled in the bootloader configuration                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.3        | Ensure AppArmor is installed, enabled, and active                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.4        | Ensure all AppArmor Profiles are in enforce or complain mode                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.5        | Ensure all AppArmor Profiles are enforcing                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.4          | Ensure permissions on /etc/motd are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.5          | Ensure permissions on /etc/issue are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.6          | Ensure permissions on /etc/issue.net are configured                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.1          | Ensure GNOME Display Manager 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"/> |
| 1.7.7          | Ensure user's session lock is enabled                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.9          | Ensure GDM autorun-never is enabled                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.10         | Ensure GDM autorun-never is not overridden                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.11         | Ensure XDCMP is not enabled                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.12         | Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.13         | Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.1          | Ensure vlock is installed                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.2          | Ensure Endpoint Security for Linux Threat Prevention is installed                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.1.1        | Ensure a single time synchronization daemon is in use                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.1        | Ensure chrony is configured with authorized timeserver                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.2        | Ensure chrony is running as user_chrony                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.3        | Ensure chrony is enabled and running                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3.1        | Ensure systemd-timesyncd configured with authorized timeserver                               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                           | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                           | Yes                      | No                       |
| 2.1.3.2        | Ensure systemd-timesyncd is enabled and running                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.1        | Ensure ntp access control is configured                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.2        | Ensure ntp is configured with authorized timeserver                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.3        | Ensure ntp is running as user ntp                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.4        | Ensure ntp is enabled and running                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.5          | Ensure system clocks are synchronize to the authoritative time source when the time difference is greater than one second | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.6          | Ensure system clocks are synchronized with a time server designated for the appropriate DoD network                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7          | Ensure system timezone is set to UTC or GMT                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.1          | Ensure X Window System is not installed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.2          | Ensure Avahi Server is not installed                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.3          | Ensure CUPS is not installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.4          | Ensure DHCP Server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.5          | Ensure LDAP server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.6          | Ensure NFS is not installed                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.7          | Ensure DNS Server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.8          | Ensure FTP Server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.9          | Ensure HTTP server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.10         | Ensure IMAP and POP3 server are not installed                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.11         | Ensure Samba is not installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.12         | Ensure HTTP Proxy Server is not installed                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.13         | Ensure SNMP Server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.14         | Ensure NIS Server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.15         | Ensure dnsmasq is not installed                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.16         | Ensure mail transfer agent is configured for local-only mode                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.17         | Ensure telnetd is not installed                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.18         | Ensure rsync service is either not installed or is masked                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.19         | Ensure rsh-server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.1          | Ensure NIS Client is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                      | Set Correctly            |                          |
|----------------|------------------------------------------------------|--------------------------|--------------------------|
|                |                                                      | Yes                      | No                       |
| 2.3.2          | Ensure rsh client is not installed                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.3          | Ensure talk client is not installed                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.4          | Ensure telnet client is not installed                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.5          | Ensure LDAP client is not installed                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.6          | Ensure RPC is not installed                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4            | Ensure nonessential services are removed or masked   | <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 sctp 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 tipc 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 tcp syn Cookies is enabled                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.9          | Ensure source routed packets are not accepted        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.10         | Ensure suspicious packets are logged                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.11         | Ensure ipv6 router advertisements are not accepted   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.1        | Ensure ufw is installed                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.2        | Ensure iptables-persistent is not installed with ufw | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.3        | Ensure ufw service is enabled                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.4        | Ensure ufw loopback traffic is configured            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.5        | Ensure ufw outbound connections are configured       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.6        | Ensure ufw firewall rules exist for all open ports   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.7        | Ensure ufw default deny firewall policy              | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                      | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                      | Yes                      | No                       |
| 3.4.1.8        | Ensure UFW rate-limits impacted network interfaces                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.1        | Ensure nftables is installed                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.2        | Ensure ufw is uninstalled or disabled with nftables                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.3        | Ensure iptables are flushed with nftables                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.4        | Ensure a nftables table exists                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.5        | Ensure nftables base chains exist                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.6        | Ensure nftables loopback traffic is configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.7        | Ensure nftables outbound and established connections are configured  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.8        | Ensure nftables default deny firewall policy                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.9        | Ensure nftables service is enabled                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.10       | Ensure nftables rules are permanent                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.1      | Ensure iptables packages are installed                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.2      | Ensure nftables is not installed with iptables                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.3      | Ensure ufw is uninstalled or disabled with iptables                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.1      | Ensure iptables default deny firewall policy                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.2      | Ensure iptables loopback traffic is configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.3      | Ensure iptables outbound and established connections are configured  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.4      | Ensure iptables firewall rules exist for all open ports              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.1      | Ensure ip6tables default deny firewall policy                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.2      | Ensure ip6tables loopback traffic is configured                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.3      | Ensure ip6tables outbound and established connections are configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.4      | Ensure ip6tables firewall rules exist for all open ports             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.2        | Ensure permissions on /etc/crontab are configured                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3        | Ensure permissions on /etc/cron.hourly are configured                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4        | Ensure permissions on /etc/cron.daily are configured                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5        | Ensure permissions on /etc/cron.weekly are configured                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.6        | Ensure permissions on /etc/cron.monthly are configured               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.7        | Ensure permissions on /etc/cron.d are configured                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.8        | Ensure crontab is restricted to authorized users                     | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                | Yes                      | No                       |
| 4.1.2.1        | Ensure at is restricted to authorized users                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.1          | Ensure SSH is installed and active                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.2          | Ensure permissions on /etc/ssh/sshd_config are configured                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.3          | Ensure permissions on SSH private host key files are configured                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.4          | Ensure permissions on SSH public host key files are configured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.5          | Ensure SSH access is limited                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.6          | Ensure SSH LogLevel is appropriate                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.7          | Ensure SSH PAM is enabled                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.8          | Ensure SSH root login is disabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.10         | Ensure SSH PermitEmptyPasswords is disabled                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.12         | Ensure SSH IgnoreRhosts is enabled                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.13         | Ensure SSH X11 forwarding is disabled                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.14         | Ensure only strong Ciphers are used                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.15         | Ensure only strong MAC algorithms are used                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.16         | Ensure only strong Key Exchange algorithms are used                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.19         | Ensure SSH MaxAuthTries is set to 4 or less                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.20         | Ensure SSH MaxStartups is configured                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.24         | Ensure network connections associated with SSH traffic are terminated after a period of inactivity                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.25         | Ensure network connections associated with SSH traffic are terminated at the end of the session or 10 minutes of inactivity    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.26         | Ensure Standard Mandatory DoD Notice and Consent Banner displayed before granting any local or remote connection to the system | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.27         | Ensure only FIPS validated MAC algorithms are used                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.28         | Ensure only FIPS validated Ciphers are used                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.29         | Ensure only FIPS validated Key Exchange algorithms are used                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.30         | Ensure X11UseLocalhost is enabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.1          | Ensure sudo is installed                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                  | Yes                      | No                       |
| 4.3.2          | Ensure sudo commands use pty                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.3          | Ensure sudo log file exists                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.4          | Ensure only users who need access to security functions are part of sudo group   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.5          | Ensure users must provide password for privilege escalation                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.6          | Ensure re-authentication for privilege escalation is not disabled globally       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.7          | Ensure sudo authentication timeout is configured correctly                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.8          | Ensure access to the su command is restricted                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.1        | Ensure new and changed passwords use pwquality                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.2        | Ensure password creation requirements are configured                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.3        | Ensure maximum number of same consecutive characters in a password is configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.4        | Ensure the number of changed characters in a new password is configured          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.5        | Ensure preventing the use of dictionary words for passwords is configured        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.6        | Ensure password includes at least one upper-case character                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.7        | Ensure password includes at least one lower-case character                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.8        | Ensure password includes at least one numeric character                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.9        | Ensure password includes at least one special character                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.10       | Ensure change of at least 8 characters when passwords are changed                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.11       | Ensure password is at least 15 characters                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.2.1        | Ensure password reuse is limited                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3.1        | Ensure lockout for failed password attempts is configured                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3.2        | Ensure lockout for three or more failed password attempts is configured          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.4.1        | Ensure strong password hashing algorithm is configured                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.4.2        | Ensure pam modules do not include nullok                                         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                    | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                    | Yes                      | No                       |
| 4.4.5.1        | Ensure PAM prohibits the use of cached authentications after one day                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.1        | Ensure the libpam-pkcs11 package is installed                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.2        | Ensure the opensc-pkcs11 is installed                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.3        | Ensure authenticated identity is mapped to the user or group account for PKI-based authentication  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.4        | Ensure smart card logins for multifactor authentication for local and network access               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.5        | Ensure certificates are validated by constructing a certification path to an accepted trust anchor | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.6        | Ensure Personal Identity Verification credentials are electronically verified                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.7        | Ensure PKI local cache of revocation data                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.7.1        | Ensure last successful account logon is displayed upon logon                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.8.1        | Ensure login delay after failed logon attempt                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.9          | Ensure all current passwords uses the configured hashing algorithm                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.1        | Ensure minimum days between password changes is configured                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.2        | Ensure password expiration is 365 days or less                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.3        | Ensure password expiration warning days is 7 or more                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.4        | Ensure inactive password lock is 30 days or less                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.5        | Ensure all users last password change date is in the past                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.6        | Ensure ENCRYPT_METHOD is SHA512                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.7        | Ensure temporary accounts expiration time of 72 hours or less                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.8        | Ensure root account is locked                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.9        | Ensure password expiration is 60 days or less                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.10       | Ensure emergency accounts are removed or disabled after 72 hours                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.11       | Ensure immediate change to a permanent password                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.2          | Ensure system accounts are secured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.3          | Ensure default group for the root account is GID 0                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                     | Set Correctly            |                          |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                     | Yes                      | No                       |
| 4.5.4          | Ensure default user umask is 027 or more restrictive                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.5          | Ensure default user shell timeout is configured                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.6          | Ensure default user umask is 077 or more restrictive                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.8          | Ensure default user shell timeout is 600 seconds or less                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure /etc/ssl/certs only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.1      | Ensure systemd-journal-remote is installed                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.2      | Ensure systemd-journal-remote is configured                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.3      | Ensure systemd-journal-remote is enabled                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.4      | Ensure journald is not configured to receive logs from a remote client                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.2        | Ensure journald service is enabled                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.3        | Ensure journald is configured to compress large log files                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.4        | Ensure journald is configured to write logfiles to persistent disk                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.5        | Ensure journald is not configured to send logs to rsyslog                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.6        | Ensure journald log rotation is configured per site policy                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.7        | Ensure journald default file permissions configured                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.1        | Ensure rsyslog is installed                                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.2        | Ensure rsyslog service is enabled                                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.3        | Ensure journald is configured to send logs to rsyslog                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.4        | Ensure rsyslog default file permissions are configured                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.5        | Ensure logging is configured                                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.6        | Ensure rsyslog is configured to send logs to a remote log host                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.7        | Ensure remote access methods are monitored                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.8        | Ensure rsyslog is not configured to receive logs from a remote client                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.1        | Ensure /var/log is owned by root                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.2        | Ensure /var/log is group-owned by syslog                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.3        | Ensure /var/log is mode 0755 or more restrictive                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.4        | Ensure all logfiles have appropriate access configured                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                            | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                            | Yes                      | No                       |
| 5.1.3.5        | Ensure /var/log/syslog is owned by syslog                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.6        | Ensure /var/log/syslog is group-owned by adm                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.7        | Ensure /var/log/syslog is 0640 or more restrictive                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.1        | Ensure auditd is installed                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.2        | Ensure auditd service is enabled and active                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.3        | Ensure auditing for processes that start prior to auditd is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.4        | Ensure audit_backlog_limit is sufficient                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.1        | Ensure audit log storage size is configured                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.2        | Ensure audit logs are not automatically deleted                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.3        | Ensure system is disabled when audit logs are full                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.4        | Ensure crontab scrip running to offload audit events of standalone systems                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.5        | Ensure shut down by default upon audit failure                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.6        | Ensure security personnel are notified when storage volume reaches 75 percent utilization                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.7        | Ensure sufficient storage capacity to store at least one week worth of audit records                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.8        | Ensure audit event multiplexor is configured to off-load audit logs onto a different system or storage media from the system being audited | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.1        | Ensure changes to system administration scope (sudoers) is collected                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.2        | Ensure actions as another user are always logged                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.3        | Ensure events that modify the sudo log file are collected                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.4        | Ensure events that modify date and time information are collected                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.5        | Ensure events that modify the system's network environment are collected                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.6        | Ensure use of privileged commands are collected                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.7        | Ensure unsuccessful file access attempts are collected                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.8        | Ensure events that modify user/group information are collected                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                 | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                 | Yes                      | No                       |
| 5.2.3.9        | Ensure discretionary access control permission modification events are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.10       | Ensure successful file system mounts are collected                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.11       | Ensure session initiation information is collected                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.12       | Ensure login and logout events are collected                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.13       | Ensure file deletion events by users are collected                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.14       | Ensure events that modify the system's Mandatory Access Controls are collected                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.15       | Ensure successful and unsuccessful attempts to use the chcon command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.16       | Ensure successful and unsuccessful attempts to use the setfacl command are recorded             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.17       | Ensure successful and unsuccessful attempts to use the chacl command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.18       | Ensure successful and unsuccessful attempts to use the usermod command are recorded             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.19       | Ensure kernel module loading unloading and modification is collected                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.20       | Ensure successful and unsuccessful uses of the su command are collected                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.21       | Ensure successful and unsuccessful uses of the chfn command are collected                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.22       | Ensure successful and unsuccessful uses of the ssh-agent command are collected                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.23       | Ensure successful and unsuccessful uses of the ssh-keysign command are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.24       | Ensure successful and unsuccessful attempts to use the fdisk command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.25       | Ensure successful and unsuccessful uses of the sudo command are recorded                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.26       | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are recorded | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.27       | Ensure successful and unsuccessful attempts to use the sudoedit command are recorded            | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                             | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                             | Yes                      | No                       |
| 5.2.3.28       | Ensure successful and unsuccessful attempts to use the crontab command are recorded         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.29       | Ensure successful and unsuccessful attempts to use the chsh command are recorded            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.30       | Ensure successful and unsuccessful attempts to use the chage command are recorded           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.31       | Ensure successful and unsuccessful attempts to use the newgrp command are recorded          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.32       | Ensure successful and unsuccessful attempts to use the gpasswd command are recorded         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.33       | Ensure successful and unsuccessful attempts to use the unix_update command are recorded     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.34       | Ensure successful and unsuccessful attempts to use the apparmor_parser command are recorded | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.35       | Ensure successful and unsuccessful attempts to use the passwd command are recorded          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.36       | Ensure the running and on disk configuration is the same                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.37       | Ensure the audit configuration is immutable                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.1        | Ensure the audit log directory is 0750 or more restrictive                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.2        | Ensure audit log files are mode 0640 or more restrictive                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.3        | Ensure audit log files are mode 0600 or more restrictive                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.4        | Ensure only authorized users own audit log files                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.5        | Ensure only authorized groups own audit log files                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.6        | Ensure audit configuration files are 640 or more restrictive                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.7        | Ensure only authorized users own audit configuration files                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.8        | Ensure only authorized groups own audit configuration files                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.9        | Ensure audit tools are 755 or more restrictive                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.10       | Ensure only authorized users own audit tools                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.11       | Ensure only authorized groups own audit tools                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.1          | Ensure AIDE is installed                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2          | Ensure aide script to check file integrity is the default                                   | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                | Yes                      | No                       |
| 5.3.3          | Ensure filesystem integrity is regularly checked                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.4          | Ensure System Administrator are notified of changes to the baseline configuration or anomalies | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.1          | Ensure permissions on /etc/passwd are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.2          | Ensure permissions on /etc/passwd- are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.3          | Ensure permissions on /etc/group are configured                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.4          | Ensure permissions on /etc/group- are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.5          | Ensure permissions on /etc/shadow are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.6          | Ensure permissions on /etc/shadow- are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.7          | Ensure permissions on /etc/gshadow are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.8          | Ensure permissions on /etc/gshadow- are configured                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.9          | Ensure permissions on /etc/shells are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.10         | Ensure permissions on /etc/opasswd are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.11         | Ensure world writable files and directories are secured                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.12         | Ensure no unowned or ungrouped files or directories exist                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.13         | Ensure SUID and SGID files are reviewed                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.14         | Ensure system command files are group-owned by root                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.15         | Ensure system command files are owned by root                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.16         | Ensure directories that contain system commands set to 0755 or more restrictive                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.17         | Ensure system library directories are group-owned by root                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.18         | Ensure system library files are group-owned by root                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.19         | Ensure system library directories are owned by root                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.20         | Ensure directories that contain system commands are owned by root                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.21         | Ensure system library files are owned by root                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.22         | Ensure directories that contain system commands are group-owned by root                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.23         | Ensure system library directories are 0755 or more restrictive                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.24         | Ensure system library files are 0755 or more restrictive                                       | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                               | Set Correctly            |                          |
|----------------|---------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                               | Yes                      | No                       |
| 6.2.1          | Ensure accounts in /etc/passwd use shadowed passwords         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2          | Ensure /etc/shadow password fields are not empty              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.4          | Ensure shadow group is empty                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.11         | Ensure local interactive user home directories are configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.12         | 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                       |
| 1.4.8          | 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"/> |
| 1.7.8          | Ensure GDM disabling automatic mounting of removable media is not overridden     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.1        | Ensure cron daemon is enabled and active                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.9          | Ensure SSH HostbasedAuthentication is disabled                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.11         | Ensure SSH PermitUserEnvironment is disabled                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.17         | Ensure SSH AllowTcpForwarding is disabled                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.18         | Ensure SSH warning banner is configured                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.21         | Ensure SSH LoginGraceTime is set to one minute or less                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.22         | Ensure SSH MaxSessions is set to 10 or less                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.23         | Ensure SSH Idle Timeout Interval is configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.7          | Ensure nologin is not listed in /etc/shells                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.5          | Ensure cryptographic mechanisms are used to protect the integrity of audit tools | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3          | Ensure all groups in /etc/passwd exist in /etc/group                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.5          | Ensure no duplicate UIDs exist                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.6          | Ensure no duplicate GIDs exist                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.7          | Ensure no duplicate user names exist                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.8          | Ensure no duplicate group names exist                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.9          | Ensure root PATH Integrity                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.10         | Ensure root is the only UID 0 account                                            | <input type="checkbox"/> | <input type="checkbox"/> |

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

|           | Recommendation                                                          | Set Correctly            |                          |
|-----------|-------------------------------------------------------------------------|--------------------------|--------------------------|
|           |                                                                         | Yes                      | No                       |
| 1.1.1.9   | Ensure usb-storage kernel module is not available                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.12  | Ensure sticky bit is set on all world-writable directories              | <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     | Ensure updates, patches, and additional security software are installed | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2     | Ensure package manager repositories are configured                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.3     | Ensure GPG keys are configured                                          | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                      | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                      | Yes                      | No                       |
| 1.2.4          | Ensure apt is configured to prevent installation without verification of a recognized and approved digital signature | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.5          | Ensure the Advance Package Tool removes all software components after updated versions have been installed           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1          | Ensure bootloader password is set                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.2          | Ensure permissions on bootloader config are configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.3          | Ensure authentication required for single user mode                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5          | Ensure maxlogins is 10 or less                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.9          | Ensure the Ctrl-Alt-Delete key sequence is disabled                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.1        | Ensure AppArmor is installed                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.2        | Ensure AppArmor is enabled in the bootloader configuration                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.4        | Ensure all AppArmor Profiles are in enforce or complain mode                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.5        | Ensure all AppArmor Profiles are enforcing                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.4          | Ensure permissions on /etc/motd are configured                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.5          | Ensure permissions on /etc/issue are configured                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.6          | Ensure permissions on /etc/issue.net are 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"/> |
| 1.7.7          | Ensure user's session lock is enabled                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.9          | Ensure GDM autorun-never is enabled                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.10         | Ensure GDM autorun-never is not overridden                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.12         | Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.13         | Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.1          | Ensure vlock is installed                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7          | Ensure system timezone is set to UTC or GMT                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.1        | Ensure ufw is installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                      | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                      | Yes                      | No                       |
| 3.4.1.2        | Ensure iptables-persistent is not installed with ufw                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.3        | Ensure ufw service is enabled                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.4        | Ensure ufw loopback traffic is configured                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.5        | Ensure ufw outbound connections are configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.6        | Ensure ufw firewall rules exist for all open ports                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.7        | Ensure ufw default deny firewall policy                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.8        | Ensure UFW rate-limits impacted network interfaces                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.1        | Ensure nftables is installed                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.2        | Ensure ufw is uninstalled or disabled with nftables                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.3        | Ensure iptables are flushed with nftables                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.4        | Ensure a nftables table exists                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.5        | Ensure nftables base chains exist                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.6        | Ensure nftables loopback traffic is configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.7        | Ensure nftables outbound and established connections are configured  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.8        | Ensure nftables default deny firewall policy                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.9        | Ensure nftables service is enabled                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.10       | Ensure nftables rules are permanent                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.1      | Ensure iptables packages are installed                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.2      | Ensure nftables is not installed with iptables                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.3      | Ensure ufw is uninstalled or disabled with iptables                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.1      | Ensure iptables default deny firewall policy                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.2      | Ensure iptables loopback traffic is configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.3      | Ensure iptables outbound and established connections are configured  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.4      | Ensure iptables firewall rules exist for all open ports              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.1      | Ensure ip6tables default deny firewall policy                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.2      | Ensure ip6tables loopback traffic is configured                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.3      | Ensure ip6tables outbound and established connections are configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.4      | Ensure ip6tables firewall rules exist for all open ports             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.2        | Ensure permissions on /etc/crontab are configured                    | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                | Yes                      | No                       |
| 4.1.1.3        | Ensure permissions on /etc/cron.hourly are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4        | Ensure permissions on /etc/cron.daily are configured                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5        | Ensure permissions on /etc/cron.weekly are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.6        | Ensure permissions on /etc/cron.monthly are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.7        | Ensure permissions on /etc/cron.d are configured                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.8        | Ensure crontab is restricted to authorized users                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.1        | Ensure at is restricted to authorized users                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.2          | Ensure permissions on /etc/ssh/sshd_config are configured                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.3          | Ensure permissions on SSH private host key files are configured                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.4          | Ensure permissions on SSH public host key files are configured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.5          | Ensure SSH access is limited                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.6          | Ensure SSH LogLevel is appropriate                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.7          | Ensure SSH PAM is enabled                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.8          | Ensure SSH root login is disabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.10         | Ensure SSH PermitEmptyPasswords is disabled                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.12         | Ensure SSH IgnoreRhosts is enabled                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.20         | Ensure SSH MaxStartups is configured                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.24         | Ensure network connections associated with SSH traffic are terminated after a period of inactivity                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.25         | Ensure network connections associated with SSH traffic are terminated at the end of the session or 10 minutes of inactivity    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.26         | Ensure Standard Mandatory DoD Notice and Consent Banner displayed before granting any local or remote connection to the system | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.30         | Ensure X11UseLocalhost is enabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.1          | Ensure sudo is installed                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.2          | Ensure sudo commands use pty                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.4          | Ensure only users who need access to security functions are part of sudo group                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                  | Yes                      | No                       |
| 4.3.5          | Ensure users must provide password for privilege escalation                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.6          | Ensure re-authentication for privilege escalation is not disabled globally       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.7          | Ensure sudo authentication timeout is configured correctly                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.8          | Ensure access to the su command is restricted                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.1        | Ensure new and changed passwords use pwquality                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.2        | Ensure password creation requirements are configured                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.3        | Ensure maximum number of same consecutive characters in a password is configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.4        | Ensure the number of changed characters in a new password is configured          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.5        | Ensure preventing the use of dictionary words for passwords is configured        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.6        | Ensure password includes at least one upper-case character                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.7        | Ensure password includes at least one lower-case character                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.8        | Ensure password includes at least one numeric character                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.9        | Ensure password includes at least one special character                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.10       | Ensure change of at least 8 characters when passwords are changed                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.11       | Ensure password is at least 15 characters                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.2.1        | Ensure password reuse is limited                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3.1        | Ensure lockout for failed password attempts is configured                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3.2        | Ensure lockout for three or more failed password attempts is configured          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.4.2        | Ensure pam modules do not include nullok                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.5.1        | Ensure PAM prohibits the use of cached authentications after one day             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.1        | Ensure the libpam-pkcs11 package is installed                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.2        | Ensure the opensc-pkcs11 is installed                                            | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                     | Set Correctly            |                          |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                     | Yes                      | No                       |
| 4.4.6.3        | Ensure authenticated identity is mapped to the user or group account for PKI-based authentication                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.4        | Ensure smart card logins for multifactor authentication for local and network access                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.5        | Ensure certificates are validated by constructing a certification path to an accepted trust anchor                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.6        | Ensure Personal Identity Verification credentials are electronically verified                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.7        | Ensure PKI local cache of revocation data                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.7.1        | Ensure last successful account logon is displayed upon logon                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.8.1        | Ensure login delay after failed logon attempt                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.1        | Ensure minimum days between password changes is configured                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.2        | Ensure password expiration is 365 days or less                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.3        | Ensure password expiration warning days is 7 or more                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.4        | Ensure inactive password lock is 30 days or less                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.5        | Ensure all users last password change date is in the past                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.7        | Ensure temporary accounts expiration time of 72 hours or less                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.8        | Ensure root account is locked                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.9        | Ensure password expiration is 60 days or less                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.10       | Ensure emergency accounts are removed or disabled after 72 hours                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.11       | Ensure immediate change to a permanent password                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.2          | Ensure system accounts are secured                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.3          | Ensure default group for the root account is GID 0                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.4          | Ensure default user umask is 027 or more restrictive                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.5          | Ensure default user shell timeout is configured                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.6          | Ensure default user umask is 077 or more restrictive                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.8          | Ensure default user shell timeout is 600 seconds or less                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure /etc/ssl/certs only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                        | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                        | Yes                      | No                       |
| 5.1.1.1.1      | Ensure systemd-journal-remote is installed                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.2      | Ensure systemd-journal-remote is configured                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.3      | Ensure systemd-journal-remote is enabled                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.4      | Ensure journald is not configured to receive logs from a remote client | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.2        | Ensure journald service is enabled                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.3        | Ensure journald is configured to compress large log files              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.4        | Ensure journald is configured to write logfiles to persistent disk     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.5        | Ensure journald is not configured to send logs to rsyslog              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.6        | Ensure journald log rotation is configured per site policy             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.7        | Ensure journald default file permissions configured                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.1        | Ensure rsyslog is installed                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.2        | Ensure rsyslog service is enabled                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.3        | Ensure journald is configured to send logs to rsyslog                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.4        | Ensure rsyslog default file permissions are configured                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.5        | Ensure logging is configured                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.6        | Ensure rsyslog is configured to send logs to a remote log host         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.7        | Ensure remote access methods are monitored                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.8        | Ensure rsyslog is not configured to receive logs from a remote client  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.1        | Ensure /var/log is owned by root                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.2        | Ensure /var/log is group-owned by syslog                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.3        | Ensure /var/log is mode 0755 or more restrictive                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.4        | Ensure all logfiles have appropriate access configured                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.5        | Ensure /var/log/syslog is owned by syslog                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.6        | Ensure /var/log/syslog is group-owned by adm                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.7        | Ensure /var/log/syslog is 0640 or more restrictive                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.2        | Ensure auditd service is enabled and active                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.3        | Ensure auditing for processes that start prior to auditd is enabled    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.4        | Ensure audit_backlog_limit is sufficient                               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                            | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                            | Yes                      | No                       |
| 5.2.2.1        | Ensure audit log storage size is configured                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.2        | Ensure audit logs are not automatically deleted                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.3        | Ensure system is disabled when audit logs are full                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.4        | Ensure crontab scrip running to offload audit events of standalone systems                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.5        | Ensure shut down by default upon audit failure                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.6        | Ensure security personnel are notified when storage volume reaches 75 percent utilization                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.7        | Ensure sufficient storage capacity to store at least one week worth of audit records                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.8        | Ensure audit event multiplexor is configured to off-load audit logs onto a different system or storage media from the system being audited | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.15       | Ensure successful and unsuccessful attempts to use the chcon command are recorded                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.16       | Ensure successful and unsuccessful attempts to use the setfacl command are recorded                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.17       | Ensure successful and unsuccessful attempts to use the chacl command are recorded                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.18       | Ensure successful and unsuccessful attempts to use the usermod command are recorded                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.20       | Ensure successful and unsuccessful uses of the su command are collected                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.21       | Ensure successful and unsuccessful uses of the chfn command are collected                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.22       | Ensure successful and unsuccessful uses of the ssh-agent command are collected                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.23       | Ensure successful and unsuccessful uses of the ssh-keysign command are collected                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.24       | Ensure successful and unsuccessful attempts to use the fdisk command are recorded                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.25       | Ensure successful and unsuccessful uses of the sudo command are recorded                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.26       | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are recorded                                            | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                             | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                             | Yes                      | No                       |
| 5.2.3.27       | Ensure successful and unsuccessful attempts to use the sudoedit command are recorded        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.28       | Ensure successful and unsuccessful attempts to use the crontab command are recorded         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.29       | Ensure successful and unsuccessful attempts to use the chsh command are recorded            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.30       | Ensure successful and unsuccessful attempts to use the chage command are recorded           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.31       | Ensure successful and unsuccessful attempts to use the newgrp command are recorded          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.32       | Ensure successful and unsuccessful attempts to use the gpasswd command are recorded         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.33       | Ensure successful and unsuccessful attempts to use the unix_update command are recorded     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.34       | Ensure successful and unsuccessful attempts to use the apparmor_parser command are recorded | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.35       | Ensure successful and unsuccessful attempts to use the passwd command are recorded          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.37       | Ensure the audit configuration is immutable                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.1        | Ensure the audit log directory is 0750 or more restrictive                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.2        | Ensure audit log files are mode 0640 or more restrictive                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.3        | Ensure audit log files are mode 0600 or more restrictive                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.4        | Ensure only authorized users own audit log files                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.5        | Ensure only authorized groups own audit log files                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.6        | Ensure audit configuration files are 640 or more restrictive                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.7        | Ensure only authorized users own audit configuration files                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.8        | Ensure only authorized groups own audit configuration files                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.9        | Ensure audit tools are 755 or more restrictive                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.10       | Ensure only authorized users own audit tools                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.11       | Ensure only authorized groups own audit tools                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2          | Ensure aide script to check file integrity is the default                                   | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                 | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                 | Yes                      | No                       |
| 6.1.1          | Ensure permissions on /etc/passwd are configured                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.2          | Ensure permissions on /etc/passwd- are configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.3          | Ensure permissions on /etc/group are configured                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.4          | Ensure permissions on /etc/group- are configured                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.5          | Ensure permissions on /etc/shadow are configured                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.6          | Ensure permissions on /etc/shadow- are configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.7          | Ensure permissions on /etc/gshadow are configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.8          | Ensure permissions on /etc/gshadow- are configured                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.9          | Ensure permissions on /etc/shells are configured                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.10         | Ensure permissions on /etc/opasswd are configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.11         | Ensure world writable files and directories are secured                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.12         | Ensure no unowned or ungrouped files or directories exist                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.13         | Ensure SUID and SGID files are reviewed                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.14         | Ensure system command files are group-owned by root                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.15         | Ensure system command files are owned by root                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.16         | Ensure directories that contain system commands set to 0755 or more restrictive | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.17         | Ensure system library directories are group-owned by root                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.18         | Ensure system library files are group-owned by root                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.19         | Ensure system library directories are owned by root                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.20         | Ensure directories that contain system commands are owned by root               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.21         | Ensure system library files are owned by root                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.22         | Ensure directories that contain system commands are group-owned by root         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.23         | Ensure system library directories are 0755 or more restrictive                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.24         | Ensure system library files are 0755 or more restrictive                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2          | Ensure /etc/shadow password fields are not empty                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.4          | Ensure shadow group is empty                                                    | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                               | Set Correctly            |                          |
|----------------|---------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                               | Yes                      | No                       |
| 6.2.11         | Ensure local interactive user home directories are configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.12         | Ensure local interactive user dot files access is configured  | <input type="checkbox"/> | <input type="checkbox"/> |

DRAFT

# 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 overlayfs kernel module is not available                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.7   | Ensure squashfs kernel module is not available                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.8   | Ensure udf kernel module is not available                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.9   | Ensure usb-storage kernel module is not available                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.10  | Ensure data-at-rest encryption is enabled                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.11  | Ensure data-at-rest employs cryptographic mechanisms to prevent unauthorized modification | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.12  | Ensure sticky bit is set on all world-writable directories                                | <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"/> |

| Recommendation |                                                                                                                      | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                      | Yes                      | No                       |
| 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          | Ensure updates, patches, and additional security software are installed                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2          | Ensure package manager repositories are configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.3          | Ensure GPG keys are configured                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.4          | Ensure apt is configured to prevent installation without verification of a recognized and approved digital signature | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.5          | Ensure the Advance Package Tool removes all software components after updated versions have been installed           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1          | Ensure bootloader password is set                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.2          | Ensure permissions on bootloader config are configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.3          | Ensure authentication required for single user mode                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.1          | Ensure XD/NX support is enabled                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.2          | Ensure address space layout randomization (ASLR) is enabled                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.3          | Ensure ptrace_scope is restricted                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5          | Ensure maxlogins is 10 or less                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.6          | Ensure Automatic Error Reporting is not enabled                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.7          | Ensure kdump service is not enabled                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.9          | Ensure the Ctrl-Alt-Delete key sequence is disabled                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.10         | Ensure dmesg_restrict is enabled                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                              | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                              | Yes                      | No                       |
| 1.5.1.1        | Ensure AppArmor is installed                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.2        | Ensure AppArmor is enabled in the bootloader configuration                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.4        | Ensure all AppArmor Profiles are in enforce or complain mode                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.5        | Ensure all AppArmor Profiles are enforcing                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.4          | Ensure permissions on /etc/motd are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.5          | Ensure permissions on /etc/issue are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.6          | Ensure permissions on /etc/issue.net are configured                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.1          | Ensure GNOME Display Manager 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"/> |
| 1.7.7          | Ensure user's session lock is enabled                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.9          | Ensure GDM autorun-never is enabled                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.10         | Ensure GDM autorun-never is not overridden                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.11         | Ensure XDCMP is not enabled                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.12         | Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.13         | Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.1          | Ensure vlock is installed                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.2          | Ensure Endpoint Security for Linux Threat Prevention is installed                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.1.1        | Ensure a single time synchronization daemon is in use                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.1        | Ensure chrony is configured with authorized timeserver                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.2        | Ensure chrony is running as user _chrony                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.3        | Ensure chrony is enabled and running                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3.1        | Ensure systemd-timesyncd configured with authorized timeserver                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3.2        | Ensure systemd-timesyncd is enabled and running                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.1        | Ensure ntp access control is configured                                                      | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                           | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                           | Yes                      | No                       |
| 2.1.4.2        | Ensure ntp is configured with authorized timeserver                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.3        | Ensure ntp is running as user ntp                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.4        | Ensure ntp is enabled and running                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.5          | Ensure system clocks are synchronize to the authoritative time source when the time difference is greater than one second | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.6          | Ensure system clocks are synchronized with a time server designated for the appropriate DoD network                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7          | Ensure system timezone is set to UTC or GMT                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.1          | Ensure X Window System is not installed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.2          | Ensure Avahi Server is not installed                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.3          | Ensure CUPS is not installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.4          | Ensure DHCP Server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.5          | Ensure LDAP server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.6          | Ensure NFS is not installed                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.7          | Ensure DNS Server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.8          | Ensure FTP Server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.9          | Ensure HTTP server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.10         | Ensure IMAP and POP3 server are not installed                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.11         | Ensure Samba is not installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.12         | Ensure HTTP Proxy Server is not installed                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.13         | Ensure SNMP Server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.14         | Ensure NIS Server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.15         | Ensure dnsmasq is not installed                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.16         | Ensure mail transfer agent is configured for local-only mode                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.17         | Ensure telnetd is not installed                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.18         | Ensure rsync service is either not installed or is masked                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.19         | Ensure rsh-server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.1          | Ensure NIS Client is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.2          | Ensure rsh client is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.3          | Ensure talk client is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                      | Set Correctly            |                          |
|----------------|------------------------------------------------------|--------------------------|--------------------------|
|                |                                                      | Yes                      | No                       |
| 2.3.4          | Ensure telnet client is not installed                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.5          | Ensure LDAP client is not installed                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.6          | Ensure RPC is not installed                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4            | Ensure nonessential services are removed or masked   | <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 sctp 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 tipc 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 tcp syn Cookies is enabled                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.9          | Ensure source routed packets are not accepted        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.10         | Ensure suspicious packets are logged                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.11         | Ensure ipv6 router advertisements are not accepted   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.1        | Ensure ufw is installed                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.2        | Ensure iptables-persistent is not installed with ufw | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.3        | Ensure ufw service is enabled                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.4        | Ensure ufw loopback traffic is configured            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.5        | Ensure ufw outbound connections are configured       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.6        | Ensure ufw firewall rules exist for all open ports   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.7        | Ensure ufw default deny firewall policy              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.8        | Ensure UFW rate-limits impacted network interfaces   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.1        | Ensure nftables is installed                         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                      | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                      | Yes                      | No                       |
| 3.4.2.2        | Ensure ufw is uninstalled or disabled with nftables                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.3        | Ensure iptables are flushed with nftables                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.4        | Ensure a nftables table exists                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.5        | Ensure nftables base chains exist                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.6        | Ensure nftables loopback traffic is configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.7        | Ensure nftables outbound and established connections are configured  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.8        | Ensure nftables default deny firewall policy                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.9        | Ensure nftables service is enabled                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.10       | Ensure nftables rules are permanent                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.1      | Ensure iptables packages are installed                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.2      | Ensure nftables is not installed with iptables                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.3      | Ensure ufw is uninstalled or disabled with iptables                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.1      | Ensure iptables default deny firewall policy                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.2      | Ensure iptables loopback traffic is configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.3      | Ensure iptables outbound and established connections are configured  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.4      | Ensure iptables firewall rules exist for all open ports              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.1      | Ensure ip6tables default deny firewall policy                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.2      | Ensure ip6tables loopback traffic is configured                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.3      | Ensure ip6tables outbound and established connections are configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.4      | Ensure ip6tables firewall rules exist for all open ports             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.2        | Ensure permissions on /etc/crontab are configured                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3        | Ensure permissions on /etc/cron.hourly are configured                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4        | Ensure permissions on /etc/cron.daily are configured                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5        | Ensure permissions on /etc/cron.weekly are configured                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.6        | Ensure permissions on /etc/cron.monthly are configured               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.7        | Ensure permissions on /etc/cron.d are configured                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.8        | Ensure crontab is restricted to authorized users                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.1        | Ensure at is restricted to authorized users                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.1          | Ensure SSH is installed and active                                   | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                | Yes                      | No                       |
| 4.2.2          | Ensure permissions on /etc/ssh/sshd_config are configured                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.3          | Ensure permissions on SSH private host key files are configured                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.4          | Ensure permissions on SSH public host key files are configured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.5          | Ensure SSH access is limited                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.6          | Ensure SSH LogLevel is appropriate                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.7          | Ensure SSH PAM is enabled                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.8          | Ensure SSH root login is disabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.10         | Ensure SSH PermitEmptyPasswords is disabled                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.12         | Ensure SSH IgnoreRhosts is enabled                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.13         | Ensure SSH X11 forwarding is disabled                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.14         | Ensure only strong Ciphers are used                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.15         | Ensure only strong MAC algorithms are used                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.16         | Ensure only strong Key Exchange algorithms are used                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.19         | Ensure SSH MaxAuthTries is set to 4 or less                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.20         | Ensure SSH MaxStartups is configured                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.24         | Ensure network connections associated with SSH traffic are terminated after a period of inactivity                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.25         | Ensure network connections associated with SSH traffic are terminated at the end of the session or 10 minutes of inactivity    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.26         | Ensure Standard Mandatory DoD Notice and Consent Banner displayed before granting any local or remote connection to the system | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.27         | Ensure only FIPS validated MAC algorithms are used                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.28         | Ensure only FIPS validated Ciphers are used                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.29         | Ensure only FIPS validated Key Exchange algorithms are used                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.30         | Ensure X11UseLocalhost is enabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.1          | Ensure sudo is installed                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.2          | Ensure sudo commands use pty                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.3          | Ensure sudo log file exists                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                  | Yes                      | No                       |
| 4.3.4          | Ensure only users who need access to security functions are part of sudo group   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.5          | Ensure users must provide password for privilege escalation                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.6          | Ensure re-authentication for privilege escalation is not disabled globally       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.7          | Ensure sudo authentication timeout is configured correctly                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.8          | Ensure access to the su command is restricted                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.1        | Ensure new and changed passwords use pwquality                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.2        | Ensure password creation requirements are configured                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.3        | Ensure maximum number of same consecutive characters in a password is configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.4        | Ensure the number of changed characters in a new password is configured          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.5        | Ensure preventing the use of dictionary words for passwords is configured        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.6        | Ensure password includes at least one upper-case character                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.7        | Ensure password includes at least one lower-case character                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.8        | Ensure password includes at least one numeric character                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.9        | Ensure password includes at least one special character                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.10       | Ensure change of at least 8 characters when passwords are changed                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.11       | Ensure password is at least 15 characters                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.2.1        | Ensure password reuse is limited                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3.1        | Ensure lockout for failed password attempts is configured                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3.2        | Ensure lockout for three or more failed password attempts is configured          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.4.1        | Ensure strong password hashing algorithm is configured                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.4.2        | Ensure pam modules do not include nullok                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.5.1        | Ensure PAM prohibits the use of cached authentications after one day             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                    | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                    | Yes                      | No                       |
| 4.4.6.1        | Ensure the libpam-pkcs11 package is installed                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.2        | Ensure the opensc-pkcs11 is installed                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.3        | Ensure authenticated identity is mapped to the user or group account for PKI-based authentication  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.4        | Ensure smart card logins for multifactor authentication for local and network access               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.5        | Ensure certificates are validated by constructing a certification path to an accepted trust anchor | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.6        | Ensure Personal Identity Verification credentials are electronically verified                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.7        | Ensure PKI local cache of revocation data                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.7.1        | Ensure last successful account logon is displayed upon logon                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.8.1        | Ensure login delay after failed logon attempt                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.9          | Ensure all current passwords uses the configured hashing algorithm                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.1        | Ensure minimum days between password changes is configured                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.2        | Ensure password expiration is 365 days or less                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.3        | Ensure password expiration warning days is 7 or more                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.4        | Ensure inactive password lock is 30 days or less                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.5        | Ensure all users last password change date is in the past                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.6        | Ensure ENCRYPT_METHOD is SHA512                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.7        | Ensure temporary accounts expiration time of 72 hours or less                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.8        | Ensure root account is locked                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.9        | Ensure password expiration is 60 days or less                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.10       | Ensure emergency accounts are removed or disabled after 72 hours                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.11       | Ensure immediate change to a permanent password                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.2          | Ensure system accounts are secured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.3          | Ensure default group for the root account is GID 0                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.4          | Ensure default user umask is 027 or more restrictive                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.5          | Ensure default user shell timeout is configured                                                    | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                     | Set Correctly            |                          |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                     | Yes                      | No                       |
| 4.5.6          | Ensure default user umask is 077 or more restrictive                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.8          | Ensure default user shell timeout is 600 seconds or less                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure /etc/ssl/certs only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.1      | Ensure systemd-journal-remote is installed                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.2      | Ensure systemd-journal-remote is configured                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.3      | Ensure systemd-journal-remote is enabled                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.4      | Ensure journald is not configured to receive logs from a remote client                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.2        | Ensure journald service is enabled                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.3        | Ensure journald is configured to compress large log files                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.4        | Ensure journald is configured to write logfiles to persistent disk                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.5        | Ensure journald is not configured to send logs to rsyslog                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.6        | Ensure journald log rotation is configured per site policy                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.7        | Ensure journald default file permissions configured                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.1        | Ensure rsyslog is installed                                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.2        | Ensure rsyslog service is enabled                                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.3        | Ensure journald is configured to send logs to rsyslog                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.4        | Ensure rsyslog default file permissions are configured                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.5        | Ensure logging is configured                                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.6        | Ensure rsyslog is configured to send logs to a remote log host                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.7        | Ensure remote access methods are monitored                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.8        | Ensure rsyslog is not configured to receive logs from a remote client                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.1        | Ensure /var/log is owned by root                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.2        | Ensure /var/log is group-owned by syslog                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.3        | Ensure /var/log is mode 0755 or more restrictive                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.4        | Ensure all logfiles have appropriate access configured                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.5        | Ensure /var/log/syslog is owned by syslog                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.6        | Ensure /var/log/syslog is group-owned by adm                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                            | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                            | Yes                      | No                       |
| 5.1.3.7        | Ensure /var/log/syslog is 0640 or more restrictive                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.1        | Ensure auditd is installed                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.2        | Ensure auditd service is enabled and active                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.3        | Ensure auditing for processes that start prior to auditd is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.4        | Ensure audit_backlog_limit is sufficient                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.1        | Ensure audit log storage size is configured                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.2        | Ensure audit logs are not automatically deleted                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.3        | Ensure system is disabled when audit logs are full                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.4        | Ensure crontab script running to offload audit events of standalone systems                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.5        | Ensure shut down by default upon audit failure                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.6        | Ensure security personnel are notified when storage volume reaches 75 percent utilization                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.7        | Ensure sufficient storage capacity to store at least one week worth of audit records                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.8        | Ensure audit event multiplexor is configured to off-load audit logs onto a different system or storage media from the system being audited | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.1        | Ensure changes to system administration scope (sudoers) is collected                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.2        | Ensure actions as another user are always logged                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.3        | Ensure events that modify the sudo log file are collected                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.4        | Ensure events that modify date and time information are collected                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.5        | Ensure events that modify the system's network environment are collected                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.6        | Ensure use of privileged commands are collected                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.7        | Ensure unsuccessful file access attempts are collected                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.8        | Ensure events that modify user/group information are collected                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.9        | Ensure discretionary access control permission modification events are collected                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.10       | Ensure successful file system mounts are collected                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                 | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                 | Yes                      | No                       |
| 5.2.3.11       | Ensure session initiation information is collected                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.12       | Ensure login and logout events are collected                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.13       | Ensure file deletion events by users are collected                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.14       | Ensure events that modify the system's Mandatory Access Controls are collected                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.15       | Ensure successful and unsuccessful attempts to use the chcon command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.16       | Ensure successful and unsuccessful attempts to use the setfacil command are recorded            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.17       | Ensure successful and unsuccessful attempts to use the chacl command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.18       | Ensure successful and unsuccessful attempts to use the usermod command are recorded             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.19       | Ensure kernel module loading unloading and modification is collected                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.20       | Ensure successful and unsuccessful uses of the su command are collected                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.21       | Ensure successful and unsuccessful uses of the chfn command are collected                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.22       | Ensure successful and unsuccessful uses of the ssh-agent command are collected                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.23       | Ensure successful and unsuccessful uses of the ssh-keysign command are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.24       | Ensure successful and unsuccessful attempts to use the fdisk command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.25       | Ensure successful and unsuccessful uses of the sudo command are recorded                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.26       | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are recorded | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.27       | Ensure successful and unsuccessful attempts to use the sudoedit command are recorded            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.28       | Ensure successful and unsuccessful attempts to use the crontab command are recorded             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.29       | Ensure successful and unsuccessful attempts to use the chsh command are recorded                | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                             | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                             | Yes                      | No                       |
| 5.2.3.30       | Ensure successful and unsuccessful attempts to use the chage command are recorded           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.31       | Ensure successful and unsuccessful attempts to use the newgrp command are recorded          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.32       | Ensure successful and unsuccessful attempts to use the gpasswd command are recorded         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.33       | Ensure successful and unsuccessful attempts to use the unix_update command are recorded     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.34       | Ensure successful and unsuccessful attempts to use the apparmor_parser command are recorded | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.35       | Ensure successful and unsuccessful attempts to use the passwd command are recorded          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.36       | Ensure the running and on disk configuration is the same                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.37       | Ensure the audit configuration is immutable                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.1        | Ensure the audit log directory is 0750 or more restrictive                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.2        | Ensure audit log files are mode 0640 or more restrictive                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.3        | Ensure audit log files are mode 0600 or more restrictive                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.4        | Ensure only authorized users own audit log files                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.5        | Ensure only authorized groups own audit log files                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.6        | Ensure audit configuration files are 640 or more restrictive                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.7        | Ensure only authorized users own audit configuration files                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.8        | Ensure only authorized groups own audit configuration files                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.9        | Ensure audit tools are 755 or more restrictive                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.10       | Ensure only authorized users own audit tools                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.11       | Ensure only authorized groups own audit tools                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2          | Ensure aide script to check file integrity is the default                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3          | Ensure filesystem integrity is regularly checked                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.1          | Ensure permissions on /etc/passwd are configured                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.2          | Ensure permissions on /etc/passwd- are configured                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.3          | Ensure permissions on /etc/group are configured                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.4          | Ensure permissions on /etc/group- are configured                                            | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                 | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                 | Yes                      | No                       |
| 6.1.5          | Ensure permissions on /etc/shadow are configured                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.6          | Ensure permissions on /etc/shadow- are configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.7          | Ensure permissions on /etc/gshadow are configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.8          | Ensure permissions on /etc/gshadow- are configured                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.9          | Ensure permissions on /etc/shells are configured                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.10         | Ensure permissions on /etc/opasswd are configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.11         | Ensure world writable files and directories are secured                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.12         | Ensure no unowned or ungrouped files or directories exist                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.13         | Ensure SUID and SGID files are reviewed                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.14         | Ensure system command files are group-owned by root                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.15         | Ensure system command files are owned by root                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.16         | Ensure directories that contain system commands set to 0755 or more restrictive | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.17         | Ensure system library directories are group-owned by root                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.18         | Ensure system library files are group-owned by root                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.19         | Ensure system library directories are owned by root                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.20         | Ensure directories that contain system commands are owned by root               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.21         | Ensure system library files are owned by root                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.22         | Ensure directories that contain system commands are group-owned by root         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.23         | Ensure system library directories are 0755 or more restrictive                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.24         | Ensure system library files are 0755 or more restrictive                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1          | Ensure accounts in /etc/passwd use shadowed passwords                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2          | Ensure /etc/shadow password fields are not empty                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.4          | Ensure shadow group is empty                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.11         | Ensure local interactive user home directories are configured                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.12         | 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 overlayfs kernel module is not available                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.7        | Ensure squashfs kernel module is not available                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.8        | Ensure udf kernel module is not available                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.9        | Ensure usb-storage kernel module is not available                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.10       | Ensure data-at-rest encryption is enabled                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.11       | Ensure data-at-rest employs cryptographic mechanisms to prevent unauthorized modification | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.12       | Ensure sticky bit is set on all world-writable directories                                | <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"/> |

| Recommendation |                                                                                                                      | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                      | Yes                      | No                       |
| 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          | Ensure updates, patches, and additional security software are installed                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2          | Ensure package manager repositories are configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.3          | Ensure GPG keys are configured                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.4          | Ensure apt is configured to prevent installation without verification of a recognized and approved digital signature | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.5          | Ensure the Advance Package Tool removes all software components after updated versions have been installed           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1          | Ensure bootloader password is set                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.2          | Ensure permissions on bootloader config are configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.3          | Ensure authentication required for single user mode                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.1          | Ensure XD/NX support is enabled                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.2          | Ensure address space layout randomization (ASLR) is enabled                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.3          | Ensure ptrace_scope is restricted                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.4          | Ensure prelink is not installed                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5          | Ensure maxlogins is 10 or less                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.6          | Ensure Automatic Error Reporting is not enabled                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.7          | Ensure kdump service is not enabled                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.9          | Ensure the Ctrl-Alt-Delete key sequence is disabled                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                              | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                              | Yes                      | No                       |
| 1.4.10         | Ensure dmesg_restrict is enabled                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.1        | Ensure AppArmor is installed                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.2        | Ensure AppArmor is enabled in the bootloader configuration                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.3        | Ensure AppArmor is installed, enabled, and active                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.4        | Ensure all AppArmor Profiles are in enforce or complain mode                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1.5        | Ensure all AppArmor Profiles are enforcing                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.4          | Ensure permissions on /etc/motd are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.5          | Ensure permissions on /etc/issue are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.6          | Ensure permissions on /etc/issue.net are configured                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.1          | Ensure GNOME Display Manager 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"/> |
| 1.7.7          | Ensure user's session lock is enabled                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.9          | Ensure GDM autorun-never is enabled                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.10         | Ensure GDM autorun-never is not overridden                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.11         | Ensure XDCMP is not enabled                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.12         | Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.13         | Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.1          | Ensure vlock is installed                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.2          | Ensure Endpoint Security for Linux Threat Prevention is installed                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.1.1        | Ensure a single time synchronization daemon is in use                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.1        | Ensure chrony is configured with authorized timeserver                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.2        | Ensure chrony is running as user_chrony                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2.3        | Ensure chrony is enabled and running                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3.1        | Ensure systemd-timesyncd configured with authorized timeserver                               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                           | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                           | Yes                      | No                       |
| 2.1.3.2        | Ensure systemd-timesyncd is enabled and running                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.1        | Ensure ntp access control is configured                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.2        | Ensure ntp is configured with authorized timeserver                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.3        | Ensure ntp is running as user ntp                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4.4        | Ensure ntp is enabled and running                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.5          | Ensure system clocks are synchronize to the authoritative time source when the time difference is greater than one second | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.6          | Ensure system clocks are synchronized with a time server designated for the appropriate DoD network                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7          | Ensure system timezone is set to UTC or GMT                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.1          | Ensure X Window System is not installed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.2          | Ensure Avahi Server is not installed                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.3          | Ensure CUPS is not installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.4          | Ensure DHCP Server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.5          | Ensure LDAP server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.6          | Ensure NFS is not installed                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.7          | Ensure DNS Server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.8          | Ensure FTP Server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.9          | Ensure HTTP server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.10         | Ensure IMAP and POP3 server are not installed                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.11         | Ensure Samba is not installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.12         | Ensure HTTP Proxy Server is not installed                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.13         | Ensure SNMP Server is not installed                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.14         | Ensure NIS Server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.15         | Ensure dnsmasq is not installed                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.16         | Ensure mail transfer agent is configured for local-only mode                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.17         | Ensure telnetd is not installed                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.18         | Ensure rsync service is either not installed or is masked                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.19         | Ensure rsh-server is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.1          | Ensure NIS Client is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                      | Set Correctly            |                          |
|----------------|------------------------------------------------------|--------------------------|--------------------------|
|                |                                                      | Yes                      | No                       |
| 2.3.2          | Ensure rsh client is not installed                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.3          | Ensure talk client is not installed                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.4          | Ensure telnet client is not installed                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.5          | Ensure LDAP client is not installed                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.6          | Ensure RPC is not installed                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4            | Ensure nonessential services are removed or masked   | <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 sctp 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 tipc 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 tcp syn Cookies is enabled                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.9          | Ensure source routed packets are not accepted        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.10         | Ensure suspicious packets are logged                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.11         | Ensure ipv6 router advertisements are not accepted   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.1        | Ensure ufw is installed                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.2        | Ensure iptables-persistent is not installed with ufw | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.3        | Ensure ufw service is enabled                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.4        | Ensure ufw loopback traffic is configured            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.5        | Ensure ufw outbound connections are configured       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.6        | Ensure ufw firewall rules exist for all open ports   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.1.7        | Ensure ufw default deny firewall policy              | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                      | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                      | Yes                      | No                       |
| 3.4.1.8        | Ensure UFW rate-limits impacted network interfaces                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.1        | Ensure nftables is installed                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.2        | Ensure ufw is uninstalled or disabled with nftables                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.3        | Ensure iptables are flushed with nftables                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.4        | Ensure a nftables table exists                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.5        | Ensure nftables base chains exist                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.6        | Ensure nftables loopback traffic is configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.7        | Ensure nftables outbound and established connections are configured  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.8        | Ensure nftables default deny firewall policy                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.9        | Ensure nftables service is enabled                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2.10       | Ensure nftables rules are permanent                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.1      | Ensure iptables packages are installed                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.2      | Ensure nftables is not installed with iptables                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.1.3      | Ensure ufw is uninstalled or disabled with iptables                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.1      | Ensure iptables default deny firewall policy                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.2      | Ensure iptables loopback traffic is configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.3      | Ensure iptables outbound and established connections are configured  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.2.4      | Ensure iptables firewall rules exist for all open ports              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.1      | Ensure ip6tables default deny firewall policy                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.2      | Ensure ip6tables loopback traffic is configured                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.3      | Ensure ip6tables outbound and established connections are configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3.3.4      | Ensure ip6tables firewall rules exist for all open ports             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.2        | Ensure permissions on /etc/crontab are configured                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3        | Ensure permissions on /etc/cron.hourly are configured                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4        | Ensure permissions on /etc/cron.daily are configured                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5        | Ensure permissions on /etc/cron.weekly are configured                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.6        | Ensure permissions on /etc/cron.monthly are configured               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.7        | Ensure permissions on /etc/cron.d are configured                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.8        | Ensure crontab is restricted to authorized users                     | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                | Yes                      | No                       |
| 4.1.2.1        | Ensure at is restricted to authorized users                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.1          | Ensure SSH is installed and active                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.2          | Ensure permissions on /etc/ssh/sshd_config are configured                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.3          | Ensure permissions on SSH private host key files are configured                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.4          | Ensure permissions on SSH public host key files are configured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.5          | Ensure SSH access is limited                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.6          | Ensure SSH LogLevel is appropriate                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.7          | Ensure SSH PAM is enabled                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.8          | Ensure SSH root login is disabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.10         | Ensure SSH PermitEmptyPasswords is disabled                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.12         | Ensure SSH IgnoreRhosts is enabled                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.13         | Ensure SSH X11 forwarding is disabled                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.14         | Ensure only strong Ciphers are used                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.15         | Ensure only strong MAC algorithms are used                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.16         | Ensure only strong Key Exchange algorithms are used                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.19         | Ensure SSH MaxAuthTries is set to 4 or less                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.20         | Ensure SSH MaxStartups is configured                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.24         | Ensure network connections associated with SSH traffic are terminated after a period of inactivity                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.25         | Ensure network connections associated with SSH traffic are terminated at the end of the session or 10 minutes of inactivity    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.26         | Ensure Standard Mandatory DoD Notice and Consent Banner displayed before granting any local or remote connection to the system | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.27         | Ensure only FIPS validated MAC algorithms are used                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.28         | Ensure only FIPS validated Ciphers are used                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.29         | Ensure only FIPS validated Key Exchange algorithms are used                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.30         | Ensure X11UseLocalhost is enabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.1          | Ensure sudo is installed                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                  | Yes                      | No                       |
| 4.3.2          | Ensure sudo commands use pty                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.3          | Ensure sudo log file exists                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.4          | Ensure only users who need access to security functions are part of sudo group   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.5          | Ensure users must provide password for privilege escalation                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.6          | Ensure re-authentication for privilege escalation is not disabled globally       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.7          | Ensure sudo authentication timeout is configured correctly                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.8          | Ensure access to the su command is restricted                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.1        | Ensure new and changed passwords use pwquality                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.2        | Ensure password creation requirements are configured                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.3        | Ensure maximum number of same consecutive characters in a password is configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.4        | Ensure the number of changed characters in a new password is configured          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.5        | Ensure preventing the use of dictionary words for passwords is configured        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.6        | Ensure password includes at least one upper-case character                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.7        | Ensure password includes at least one lower-case character                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.8        | Ensure password includes at least one numeric character                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.9        | Ensure password includes at least one special character                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.10       | Ensure change of at least 8 characters when passwords are changed                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.1.11       | Ensure password is at least 15 characters                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.2.1        | Ensure password reuse is limited                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3.1        | Ensure lockout for failed password attempts is configured                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3.2        | Ensure lockout for three or more failed password attempts is configured          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.4.1        | Ensure strong password hashing algorithm is configured                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.4.2        | Ensure pam modules do not include nullok                                         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                    | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                    | Yes                      | No                       |
| 4.4.5.1        | Ensure PAM prohibits the use of cached authentications after one day                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.1        | Ensure the libpam-pkcs11 package is installed                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.2        | Ensure the opensc-pkcs11 is installed                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.3        | Ensure authenticated identity is mapped to the user or group account for PKI-based authentication  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.4        | Ensure smart card logins for multifactor authentication for local and network access               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.5        | Ensure certificates are validated by constructing a certification path to an accepted trust anchor | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.6        | Ensure Personal Identity Verification credentials are electronically verified                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6.7        | Ensure PKI local cache of revocation data                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.7.1        | Ensure last successful account logon is displayed upon logon                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.8.1        | Ensure login delay after failed logon attempt                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.9          | Ensure all current passwords uses the configured hashing algorithm                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.1        | Ensure minimum days between password changes is configured                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.2        | Ensure password expiration is 365 days or less                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.3        | Ensure password expiration warning days is 7 or more                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.4        | Ensure inactive password lock is 30 days or less                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.5        | Ensure all users last password change date is in the past                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.6        | Ensure ENCRYPT_METHOD is SHA512                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.7        | Ensure temporary accounts expiration time of 72 hours or less                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.8        | Ensure root account is locked                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.9        | Ensure password expiration is 60 days or less                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.10       | Ensure emergency accounts are removed or disabled after 72 hours                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.1.11       | Ensure immediate change to a permanent password                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.2          | Ensure system accounts are secured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.3          | Ensure default group for the root account is GID 0                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                     | Set Correctly            |                          |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                     | Yes                      | No                       |
| 4.5.4          | Ensure default user umask is 027 or more restrictive                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.5          | Ensure default user shell timeout is configured                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.6          | Ensure default user umask is 077 or more restrictive                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.8          | Ensure default user shell timeout is 600 seconds or less                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure /etc/ssl/certs only contains certificate files whose sha256 fingerprint match the fingerprint of DoD PKI-established certificate authorities | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.1      | Ensure systemd-journal-remote is installed                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.2      | Ensure systemd-journal-remote is configured                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.3      | Ensure systemd-journal-remote is enabled                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.1.4      | Ensure journald is not configured to receive logs from a remote client                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.2        | Ensure journald service is enabled                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.3        | Ensure journald is configured to compress large log files                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.4        | Ensure journald is configured to write logfiles to persistent disk                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.5        | Ensure journald is not configured to send logs to rsyslog                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.6        | Ensure journald log rotation is configured per site policy                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1.7        | Ensure journald default file permissions configured                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.1        | Ensure rsyslog is installed                                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.2        | Ensure rsyslog service is enabled                                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.3        | Ensure journald is configured to send logs to rsyslog                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.4        | Ensure rsyslog default file permissions are configured                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.5        | Ensure logging is configured                                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.6        | Ensure rsyslog is configured to send logs to a remote log host                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.7        | Ensure remote access methods are monitored                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2.8        | Ensure rsyslog is not configured to receive logs from a remote client                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.1        | Ensure /var/log is owned by root                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.2        | Ensure /var/log is group-owned by syslog                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.3        | Ensure /var/log is mode 0755 or more restrictive                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.4        | Ensure all logfiles have appropriate access configured                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                            | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                            | Yes                      | No                       |
| 5.1.3.5        | Ensure /var/log/syslog is owned by syslog                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.6        | Ensure /var/log/syslog is group-owned by adm                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3.7        | Ensure /var/log/syslog is 0640 or more restrictive                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.1        | Ensure auditd is installed                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.2        | Ensure auditd service is enabled and active                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.3        | Ensure auditing for processes that start prior to auditd is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1.4        | Ensure audit_backlog_limit is sufficient                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.1        | Ensure audit log storage size is configured                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.2        | Ensure audit logs are not automatically deleted                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.3        | Ensure system is disabled when audit logs are full                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.4        | Ensure crontab scrip running to offload audit events of standalone systems                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.5        | Ensure shut down by default upon audit failure                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.6        | Ensure security personnel are notified when storage volume reaches 75 percent utilization                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.7        | Ensure sufficient storage capacity to store at least one week worth of audit records                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2.8        | Ensure audit event multiplexor is configured to off-load audit logs onto a different system or storage media from the system being audited | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.1        | Ensure changes to system administration scope (sudoers) is collected                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.2        | Ensure actions as another user are always logged                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.3        | Ensure events that modify the sudo log file are collected                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.4        | Ensure events that modify date and time information are collected                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.5        | Ensure events that modify the system's network environment are collected                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.6        | Ensure use of privileged commands are collected                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.7        | Ensure unsuccessful file access attempts are collected                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.8        | Ensure events that modify user/group information are collected                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                 | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                 | Yes                      | No                       |
| 5.2.3.9        | Ensure discretionary access control permission modification events are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.10       | Ensure successful file system mounts are collected                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.11       | Ensure session initiation information is collected                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.12       | Ensure login and logout events are collected                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.13       | Ensure file deletion events by users are collected                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.14       | Ensure events that modify the system's Mandatory Access Controls are collected                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.15       | Ensure successful and unsuccessful attempts to use the chcon command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.16       | Ensure successful and unsuccessful attempts to use the setfacil command are recorded            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.17       | Ensure successful and unsuccessful attempts to use the chacl command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.18       | Ensure successful and unsuccessful attempts to use the usermod command are recorded             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.19       | Ensure kernel module loading unloading and modification is collected                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.20       | Ensure successful and unsuccessful uses of the su command are collected                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.21       | Ensure successful and unsuccessful uses of the chfn command are collected                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.22       | Ensure successful and unsuccessful uses of the ssh-agent command are collected                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.23       | Ensure successful and unsuccessful uses of the ssh-keysign command are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.24       | Ensure successful and unsuccessful attempts to use the fdisk command are recorded               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.25       | Ensure successful and unsuccessful uses of the sudo command are recorded                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.26       | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are recorded | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.27       | Ensure successful and unsuccessful attempts to use the sudoedit command are recorded            | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                             | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                             | Yes                      | No                       |
| 5.2.3.28       | Ensure successful and unsuccessful attempts to use the crontab command are recorded         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.29       | Ensure successful and unsuccessful attempts to use the chsh command are recorded            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.30       | Ensure successful and unsuccessful attempts to use the chage command are recorded           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.31       | Ensure successful and unsuccessful attempts to use the newgrp command are recorded          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.32       | Ensure successful and unsuccessful attempts to use the gpasswd command are recorded         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.33       | Ensure successful and unsuccessful attempts to use the unix_update command are recorded     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.34       | Ensure successful and unsuccessful attempts to use the apparmor_parser command are recorded | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.35       | Ensure successful and unsuccessful attempts to use the passwd command are recorded          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.36       | Ensure the running and on disk configuration is the same                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3.37       | Ensure the audit configuration is immutable                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.1        | Ensure the audit log directory is 0750 or more restrictive                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.2        | Ensure audit log files are mode 0640 or more restrictive                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.3        | Ensure audit log files are mode 0600 or more restrictive                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.4        | Ensure only authorized users own audit log files                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.5        | Ensure only authorized groups own audit log files                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.6        | Ensure audit configuration files are 640 or more restrictive                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.7        | Ensure only authorized users own audit configuration files                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.8        | Ensure only authorized groups own audit configuration files                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.9        | Ensure audit tools are 755 or more restrictive                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.10       | Ensure only authorized users own audit tools                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4.11       | Ensure only authorized groups own audit tools                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.1          | Ensure AIDE is installed                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2          | Ensure aide script to check file integrity is the default                                   | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                | Yes                      | No                       |
| 5.3.3          | Ensure filesystem integrity is regularly checked                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.4          | Ensure System Administrator are notified of changes to the baseline configuration or anomalies | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.1          | Ensure permissions on /etc/passwd are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.2          | Ensure permissions on /etc/passwd- are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.3          | Ensure permissions on /etc/group are configured                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.4          | Ensure permissions on /etc/group- are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.5          | Ensure permissions on /etc/shadow are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.6          | Ensure permissions on /etc/shadow- are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.7          | Ensure permissions on /etc/gshadow are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.8          | Ensure permissions on /etc/gshadow- are configured                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.9          | Ensure permissions on /etc/shells are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.10         | Ensure permissions on /etc/opasswd are configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.11         | Ensure world writable files and directories are secured                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.12         | Ensure no unowned or ungrouped files or directories exist                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.13         | Ensure SUID and SGID files are reviewed                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.14         | Ensure system command files are group-owned by root                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.15         | Ensure system command files are owned by root                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.16         | Ensure directories that contain system commands set to 0755 or more restrictive                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.17         | Ensure system library directories are group-owned by root                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.18         | Ensure system library files are group-owned by root                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.19         | Ensure system library directories are owned by root                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.20         | Ensure directories that contain system commands are owned by root                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.21         | Ensure system library files are owned by root                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.22         | Ensure directories that contain system commands are group-owned by root                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.23         | Ensure system library directories are 0755 or more restrictive                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.24         | Ensure system library files are 0755 or more restrictive                                       | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                               | Set Correctly            |                          |
|----------------|---------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                               | Yes                      | No                       |
| 6.2.1          | Ensure accounts in /etc/passwd use shadowed passwords         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2          | Ensure /etc/shadow password fields are not empty              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.4          | Ensure shadow group is empty                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.11         | Ensure local interactive user home directories are configured | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.12         | 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                       |
| 1.4.8          | 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"/> |
| 1.7.8          | Ensure GDM disabling automatic mounting of removable media is not overridden     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.1        | Ensure cron daemon is enabled and active                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.9          | Ensure SSH HostbasedAuthentication is disabled                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.11         | Ensure SSH PermitUserEnvironment is disabled                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.17         | Ensure SSH AllowTcpForwarding is disabled                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.18         | Ensure SSH warning banner is configured                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.21         | Ensure SSH LoginGraceTime is set to one minute or less                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.22         | Ensure SSH MaxSessions is set to 10 or less                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.23         | Ensure SSH Idle Timeout Interval is configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5.7          | Ensure nologin is not listed in /etc/shells                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.5          | Ensure cryptographic mechanisms are used to protect the integrity of audit tools | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3          | Ensure all groups in /etc/passwd exist in /etc/group                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.5          | Ensure no duplicate UIDs exist                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.6          | Ensure no duplicate GIDs exist                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.7          | Ensure no duplicate user names exist                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.8          | Ensure no duplicate group names exist                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.9          | Ensure root PATH Integrity                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.10         | Ensure root is the only UID 0 account                                            | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: Change History

| Date              | Version | Changes for this version |
|-------------------|---------|--------------------------|
| 07 September 2023 | 1.0.0   | Published                |

DRAFT