

**CIS SUSE Linux Enterprise 15 Benchmark**

v1.1.1 - 01-24-2022

[http://benchmarks.cisecurity.org](http://benchmarks.cisecurity.org/)

**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/*](https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/)



1 | P a g e

Table of Contents

[Terms of Use](#page2) [1](#page2)

[Overview](#page13) [12](#page13)

[Intended Audience](#page13) [12](#page13)

[Consensus Guidance](#page13) [12](#page13)

[Typographical Conventions](#page14) [13](#page14)

[Assessment Status](#page14) [13](#page14)

[Profile Definitions](#page15) [14](#page15)

[Acknowledgements](#page16) [15](#page16)

[Recommendations](#page17) [16](#page17)

[1 Initial Setup](#page17) [16](#page17)

[1.1 Filesystem Configuration](#page18) [17](#page18)

[1.1.1 Disable unused filesystems](#page19) [18](#page19)

[1.1.1.1 Ensure mounting of squashfs filesystems is disabled (Automated)](#page20) [19](#page20)

[1.1.1.2 Ensure mounting of udf filesystems is disabled (Automated)](#page22) [21](#page22)

[1.1.1.3 Ensure mounting of FAT filesystems is limited (Automated)](#page24) [23](#page24)

[1.1.2 Ensure /tmp is configured (Automated)](#page27) [26](#page27)

[1.1.3 Ensure noexec option set on /tmp partition (Automated)](#page32) [31](#page32)

[1.1.4 Ensure nodev option set on /tmp partition (Automated)](#page35) [34](#page35)

[1.1.5 Ensure nosuid option set on /tmp partition (Automated)](#page38) [37](#page38)

[1.1.6 Ensure /dev/shm is configured (Automated)](#page41) [40](#page41)

[1.1.7 Ensure noexec option set on /dev/shm partition (Automated)](#page43) [42](#page43)

[1.1.8 Ensure nodev option set on /dev/shm partition (Automated)](#page45) [44](#page45)

[1.1.9 Ensure nosuid option set on /dev/shm partition (Automated)](#page47) [46](#page47)

[1.1.10 Ensure separate partition exists for /var (Automated)](#page49) [48](#page49)

[1.1.11 Ensure separate partition exists for /var/tmp (Automated)](#page51) [50](#page51)

[1.1.12 Ensure noexec option set on /var/tmp partition (Automated)](#page53) [52](#page53)

[1.1.13 Ensure nodev option set on /var/tmp partition (Automated)](#page55) [54](#page55)

[1.1.14 Ensure nosuid option set on /var/tmp partition (Automated)](#page57) [56](#page57)

[1.1.15 Ensure separate partition exists for /var/log (Automated)](#page59) [58](#page59)

[1.1.16 Ensure separate partition exists for /var/log/audit (Automated)](#page61) [60](#page61)

[1.1.17 Ensure separate partition exists for /home (Automated)](#page63) [62](#page63)

[1.1.18 Ensure nodev option set on /home partition (Automated)](#page65) [64](#page65)

[1.1.19 Ensure noexec option set on removable media partitions (Manual)](#page67) [66](#page67)

[1.1.20 Ensure nodev option set on removable media partitions (Manual)](#page69) [68](#page69)



2 | P a g e

[1.1.21 Ensure nosuid option set on removable media partitions (Manual)](#page70) [69](#page70)

[1.1.22 Ensure sticky bit is set on all world-writable directories (Automated)](#page71) [70](#page71)

[1.1.23 Disable Automounting (Automated)](#page73) [72](#page73)

[1.2 Configure Software Updates](#page75) [74](#page75)

[1.2.1 Ensure GPG keys are configured (Manual)](#page76) [75](#page76)

[1.2.2 Ensure package manager repositories are configured (Manual)](#page77) [76](#page77)

[1.2.3 Ensure gpgcheck is globally activated (Automated)](#page78) [77](#page78)

[1.3 Configure sudo](#page80) [79](#page80)

[1.3.1 Ensure sudo is installed (Automated)](#page81) [80](#page81)

[1.3.2 Ensure sudo commands use pty (Automated)](#page83) [82](#page83)

[1.3.3 Ensure sudo log file exists (Automated)](#page85) [84](#page85)

[1.4 Filesystem Integrity Checking](#page87) [86](#page87)

[1.4.1 Ensure AIDE is installed (Automated)](#page88) [87](#page88)

[1.4.2 Ensure filesystem integrity is regularly checked (Automated)](#page90) [89](#page90)

[1.5 Secure Boot Settings](#page93) [92](#page93)

[1.5.1 Ensure bootloader password is set (Automated)](#page94) [93](#page94)

[1.5.2 Ensure permissions on bootloader config are configured (Automated)](#page97) [96](#page97)

[1.5.3 Ensure authentication required for single user mode (Automated)](#page99) [98](#page99)

[1.6 Additional Process Hardening](#page101) [100](#page101)

[1.6.1 Ensure core dumps are restricted (Automated)](#page102) [101](#page102)

[1.6.2 Ensure XD/NX support is enabled (Automated)](#page104) [103](#page104)

[1.6.3 Ensure address space layout randomization (ASLR) is enabled (Automated)](#page106)

[105](#page106)

[1.6.4 Ensure prelink is disabled (Automated)](#page108) [107](#page108)

[1.7 Mandatory Access Control](#page110) [109](#page110)

[1.7.1 Configure AppArmor](#page111) [110](#page111)

[1.7.1.1 Ensure AppArmor is installed (Automated)](#page112) [111](#page112)

[1.7.1.2 Ensure AppArmor is enabled in the bootloader configuration (Automated)](#page114)

[113](#page114)

[1.7.1.3 Ensure all AppArmor Profiles are in enforce or complain mode](#page116)

[(Automated)](#page116) [115](#page116)

[1.7.1.4 Ensure all AppArmor Profiles are enforcing (Automated)](#page118) [117](#page118)

[1.8 Warning Banners](#page120) [119](#page120)

[1.8.1 Command Line Warning Banners](#page121) [120](#page121)

[1.8.1.1 Ensure message of the day is configured properly (Automated)](#page122) [121](#page122)



3 | P a g e

[1.8.1.2 Ensure local login warning banner is configured properly (Automated) 123](#page124)

[1.8.1.3 Ensure remote login warning banner is configured properly (Automated)](#page126)

[125](#page126)

[1.8.1.4 Ensure permissions on /etc/motd are configured (Automated)](#page128) [127](#page128)

[1.8.1.5 Ensure permissions on /etc/issue are configured (Automated)](#page129) [128](#page129)

[1.8.1.6 Ensure permissions on /etc/issue.net are configured (Automated)](#page130) [129](#page130)

[1.9 Ensure updates, patches, and additional security software are installed](#page131)

[(Manual)](#page131) [130](#page131)

[1.10 Ensure GDM is removed or login is configured (Automated)](#page133) [132](#page133)

[2 Services](#page137) [136](#page137)

[2.1 inetd Services](#page138) [137](#page138)

[2.1.1 Ensure xinetd is not installed (Automated)](#page139) [138](#page139)

[2.2 Special Purpose Services](#page141) [140](#page141)

[2.2.1 Time Synchronization](#page142) [141](#page142)

[2.2.1.1 Ensure time synchronization is in use (Automated)](#page143) [142](#page143)

[2.2.1.2 Ensure systemd-timesyncd is configured (Manual)](#page145) [144](#page145)

[2.2.1.3 Ensure chrony is configured (Automated)](#page148) [147](#page148)

[2.2.2 Ensure X11 Server components are not installed (Automated)](#page150) [149](#page150)

[2.2.3 Ensure Avahi Server is not installed (Automated)](#page151) [150](#page151)

[2.2.4 Ensure CUPS is not installed (Automated)](#page152) [151](#page152)

[2.2.5 Ensure DHCP Server is not installed (Automated)](#page154) [153](#page154)

[2.2.6 Ensure LDAP server is not installed (Automated)](#page155) [154](#page155)

[2.2.7 Ensure nfs-utils is not installed or the nfs-server service is masked](#page157)

[(Automated)](#page157) [156](#page157)

[2.2.8 Ensure rpcbind is not installed or the rpcbind services are masked](#page159)

[(Automated)](#page159) [158](#page159)

[2.2.9 Ensure DNS Server is not installed (Automated)](#page162) [161](#page162)

[2.2.10 Ensure FTP Server is not installed (Automated)](#page163) [162](#page163)

[2.2.11 Ensure HTTP server is not installed (Automated)](#page164) [163](#page164)

[2.2.12 Ensure IMAP and POP3 server is not installed (Automated)](#page165) [164](#page165)

[2.2.13 Ensure Samba is not installed (Automated)](#page167) [166](#page167)

[2.2.14 Ensure HTTP Proxy Server is not installed (Automated)](#page168) [167](#page168)

[2.2.15 Ensure net-snmp is not installed (Automated)](#page169) [168](#page169)

[2.2.16 Ensure mail transfer agent is configured for local-only mode (Automated)](#page171)

[170](#page171)



4 | P a g e

[2.2.17 Ensure rsync is not installed or the rsyncd service is masked (Automated)](#page173)

[172](#page173)

[2.2.18 Ensure NIS server is not installed (Automated)](#page175) [174](#page175)

[2.2.19 Ensure telnet-server is not installed (Automated)](#page177) [176](#page177)

[2.3 Service Clients](#page178) [177](#page178)

[2.3.1 Ensure NIS Client is not installed (Automated)](#page179) [178](#page179)

[2.3.2 Ensure rsh client is not installed (Automated)](#page181) [180](#page181)

[2.3.3 Ensure talk client is not installed (Automated)](#page183) [182](#page183)

[2.3.4 Ensure telnet client is not installed (Automated)](#page185) [184](#page185)

[2.3.5 Ensure LDAP client is not installed (Automated)](#page187) [186](#page187)

[2.4 Ensure nonessential services are removed or masked (Manual)](#page188) [187](#page188)

[3 Network Configuration](#page190) [189](#page190)

[3.1 Disable unused network protocols and devices](#page191) [190](#page191)

[3.1.1 Disable IPv6 (Automated)](#page192) [191](#page192)

[3.1.2 Ensure wireless interfaces are disabled (Manual)](#page195) [194](#page195)

[3.2 Network Parameters (Host Only)](#page197) [196](#page197)

[3.2.1 Ensure IP forwarding is disabled (Automated)](#page198) [197](#page198)

[3.2.2 Ensure packet redirect sending is disabled (Automated)](#page201) [200](#page201)

[3.3 Network Parameters (Host and Router)](#page203) [202](#page203)

[3.3.1 Ensure source routed packets are not accepted (Automated)](#page204) [203](#page204)

[3.3.2 Ensure ICMP redirects are not accepted (Automated)](#page208) [207](#page208)

[3.3.3 Ensure secure ICMP redirects are not accepted (Automated)](#page212) [211](#page212)

[3.3.4 Ensure suspicious packets are logged (Automated)](#page214) [213](#page214)

[3.3.5 Ensure broadcast ICMP requests are ignored (Automated)](#page216) [215](#page216)

[3.3.6 Ensure bogus ICMP responses are ignored (Automated)](#page218) [217](#page218)

[3.3.7 Ensure Reverse Path Filtering is enabled (Automated)](#page220) [219](#page220)

[3.3.8 Ensure TCP SYN Cookies is enabled (Automated)](#page222) [221](#page222)

[3.3.9 Ensure IPv6 router advertisements are not accepted (Automated)](#page224) [223](#page224)

[3.4 Uncommon Network Protocols](#page227) [226](#page227)

[3.4.1 Ensure DCCP is disabled (Automated)](#page228) [227](#page228)

[3.4.2 Ensure SCTP is disabled (Automated)](#page230) [229](#page230)

[3.5 Firewall Configuration](#page232) [231](#page232)

[3.5.1 Configure firewalld](#page233) [232](#page233)

[3.5.1.1 Ensure FirewallD is installed (Automated)](#page234) [233](#page234)

[3.5.1.2 Ensure nftables is not installed or stopped and masked (Automated)](#page236) [235](#page236)



5 | P a g e

[3.5.1.3 Ensure firewalld service is enabled and running (Automated)](#page238) [237](#page238)

[3.5.1.4 Ensure default zone is set (Automated)](#page240) [239](#page240)

[3.5.1.5 Ensure network interfaces are assigned to appropriate zone (Manual) .. 241](#page242)

[3.5.1.6 Ensure unnecessary services and ports are not accepted (Manual)](#page244) [243](#page244)

[3.5.2 Configure nftables](#page246) [245](#page246)

[3.5.2.1 Ensure nftables is installed (Automated)](#page250) [249](#page250)

[3.5.2.2 Ensure firewalld is not installed or stopped and masked (Automated)](#page252) [251](#page252)

[3.5.2.3 Ensure iptables are flushed (Manual)](#page254) [253](#page254)

[3.5.2.4 Ensure a table exists (Automated)](#page256) [255](#page256)

[3.5.2.5 Ensure base chains exist (Automated)](#page258) [257](#page258)

[3.5.2.6 Ensure loopback traffic is configured (Automated)](#page260) [259](#page260)

[3.5.2.7 Ensure outbound and established connections are configured (Manual)262](#page263)

[3.5.2.8 Ensure default deny firewall policy (Automated)](#page265) [264](#page265)

[3.5.2.9 Ensure nftables service is enabled (Automated)](#page267) [266](#page267)

[3.5.2.10 Ensure nftables rules are permanent (Automated)](#page268) [267](#page268)

[3.5.3 Configure iptables](#page271) [270](#page271)

[3.5.3.1.1 Ensure iptables package is installed (Automated)](#page273) [272](#page273)

[3.5.3.1.2 Ensure nftables is not installed (Automated)](#page274) [273](#page274)

[3.5.3.1.3 Ensure firewalld is not installed or stopped and masked (Automated) 274](#page275)

[3.5.3.2.1 Ensure default deny firewall policy (Automated)](#page279) [278](#page279)

[3.5.3.2.2 Ensure loopback traffic is configured (Automated)](#page280) [279](#page280)

[3.5.3.2.3 Ensure outbound and established connections are configured (Manual)](#page282)

[281](#page282)

[3.5.3.2.4 Ensure firewall rules exist for all open ports (Automated)](#page284) [283](#page284)

[3.5.3.3.1 Ensure IPv6 default deny firewall policy (Automated)](#page289) [288](#page289)

[3.5.3.3.2 Ensure IPv6 loopback traffic is configured (Automated)](#page292) [291](#page292)

[3.5.3.3.3 Ensure IPv6 outbound and established connections are configured](#page295)

[(Manual)](#page295) [294](#page295)

[3.5.3.3.4 Ensure IPv6 firewall rules exist for all open ports (Manual)](#page298) [297](#page298)

[4 Logging and Auditing](#page301) [300](#page301)

[4.1 Configure System Accounting (auditd)](#page302) [301](#page302)

[4.1.1 Ensure auditing is enabled](#page303) [302](#page303)

[4.1.1.1 Ensure auditd is installed (Automated)](#page304) [303](#page304)

[4.1.1.2 Ensure auditd service is enabled and running (Automated)](#page305) [304](#page305)



6 | P a g e

[4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled](#page307)

[(Automated)](#page307) [306](#page307)

[4.1.2 Configure Data Retention](#page309) [308](#page309)

[4.1.2.1 Ensure audit log storage size is configured (Automated)](#page310) [309](#page310)

[4.1.2.2 Ensure audit logs are not automatically deleted (Automated)](#page312) [311](#page312)

[4.1.2.3 Ensure system is disabled when audit logs are full (Automated)](#page313) [312](#page313)

[4.1.2.4 Ensure audit\_backlog\_limit is sufficient (Automated)](#page315) [314](#page315)

[4.1.3 Ensure events that modify date and time information are collected](#page317)

[(Automated)](#page317) [316](#page317)

[4.1.4 Ensure events that modify user/group information are collected](#page320)

[(Automated)](#page320) [319](#page320)

[4.1.5 Ensure events that modify the system's network environment are collected](#page322)

[(Automated)](#page322) [321](#page322)

[4.1.6 Ensure events that modify the system's Mandatory Access Controls are](#page327)

[collected (Automated)](#page327) [326](#page327)

[4.1.7 Ensure login and logout events are collected (Automated)](#page329) [328](#page329)

[4.1.8 Ensure session initiation information is collected (Automated)](#page332) [331](#page332)

[4.1.9 Ensure discretionary access control permission modification events are](#page335)

[collected (Automated)](#page335) [334](#page335)

[4.1.10 Ensure unsuccessful unauthorized file access attempts are collected](#page339)

[(Automated)](#page339) [338](#page339)

[4.1.11 Ensure use of privileged commands is collected (Automated)](#page343) [342](#page343)

[4.1.12 Ensure successful file system mounts are collected (Automated)](#page345) [344](#page345)

[4.1.13 Ensure file deletion events by users are collected (Automated)](#page348) [347](#page348)

[4.1.14 Ensure changes to system administration scope (sudoers) is collected](#page351)

[(Automated)](#page351) [350](#page351)

[4.1.15 Ensure system administrator actions (sudolog) are collected (Automated)](#page353)

[352](#page353)

[4.1.16 Ensure kernel module loading and unloading is collected (Automated) .. 354](#page355)

[4.1.17 Ensure the audit configuration is immutable (Automated)](#page358) [357](#page358)

[4.2 Configure Logging](#page360) [359](#page360)

[4.2.1 Configure rsyslog](#page361) [360](#page361)

[4.2.1.1 Ensure rsyslog is installed (Automated)](#page362) [361](#page362)

[4.2.1.2 Ensure rsyslog Service is enabled and running (Automated)](#page364) [363](#page364)

[4.2.1.3 Ensure rsyslog default file permissions configured (Automated)](#page366) [365](#page366)

[4.2.1.4 Ensure logging is configured (Manual)](#page368) [367](#page368)



7 | P a g e

[4.2.1.5 Ensure rsyslog is configured to send logs to a remote log host (Automated)](#page370)

[369](#page370)

[4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log](#page372)

[hosts. (Manual)](#page372) [371](#page372)

[4.2.2 Configure journald](#page374) [373](#page374)

[4.2.2.1 Ensure journald is configured to send logs to rsyslog (Automated)](#page375) [374](#page375)

[4.2.2.2 Ensure journald is configured to compress large log files (Automated) .. 376](#page377)

[4.2.2.3 Ensure journald is configured to write logfiles to persistent disk](#page379)

[(Automated)](#page379) [378](#page379)

[4.2.3 Ensure permissions on all logfiles are configured (Automated)](#page381) [380](#page381)

[4.2.4 Ensure logrotate is configured (Manual)](#page382) [381](#page382)

[5 Access, Authentication and Authorization](#page382) [381](#page382)

[5.1 Configure time-based job schedulers](#page384) [383](#page384)

[5.1.1 Ensure cron daemon is enabled and running (Automated)](#page385) [384](#page385)

[5.1.2 Ensure permissions on /etc/crontab are configured (Automated)](#page386) [385](#page386)

[5.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)](#page388) [387](#page388)

[5.1.4 Ensure permissions on /etc/cron.daily are configured (Automated)](#page390) [389](#page390)

[5.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated)](#page392) [391](#page392)

[5.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated)](#page394) [393](#page394)

[5.1.7 Ensure permissions on /etc/cron.d are configured (Automated)](#page396) [395](#page396)

[5.1.8 Ensure cron is restricted to authorized users (Automated)](#page398) [397](#page398)

[5.1.9 Ensure at is restricted to authorized users (Automated)](#page400) [399](#page400)

[5.2 Configure SSH Server](#page402) [401](#page402)

[5.2.1 Ensure permissions on /etc/ssh/sshd\_config are configured (Automated)](#page403)

[402](#page403)

[5.2.2 Ensure permissions on SSH private host key files are configured](#page404)

[(Automated)](#page404) [403](#page404)

[5.2.3 Ensure permissions on SSH public host key files are configured (Automated)](#page407)

[406](#page407)

[5.2.4 Ensure SSH access is limited (Automated)](#page410) [409](#page410)

[5.2.5 Ensure SSH LogLevel is appropriate (Automated)](#page412) [411](#page412)

[5.2.6 Ensure SSH X11 forwarding is disabled (Automated)](#page414) [413](#page414)

[5.2.7 Ensure SSH MaxAuthTries is set to 4 or less (Automated)](#page415) [414](#page415)

[5.2.8 Ensure SSH IgnoreRhosts is enabled (Automated)](#page416) [415](#page416)

[5.2.9 Ensure SSH HostbasedAuthentication is disabled (Automated)](#page417) [416](#page417)

[5.2.10 Ensure SSH root login is disabled (Automated)](#page418) [417](#page418)



8 | P a g e

[5.2.11 Ensure SSH PermitEmptyPasswords is disabled (Automated)](#page419) [418](#page419)

[5.2.12 Ensure SSH PermitUserEnvironment is disabled (Automated)](#page420) [419](#page420)

[5.2.13 Ensure only strong Ciphers are used (Automated)](#page421) [420](#page421)

[5.2.14 Ensure only strong MAC algorithms are used (Automated)](#page424) [423](#page424)

[5.2.15 Ensure only strong Key Exchange algorithms are used (Automated)](#page427) [426](#page427)

[5.2.16 Ensure SSH Idle Timeout Interval is configured (Automated)](#page429) [428](#page429)

[5.2.17 Ensure SSH LoginGraceTime is set to one minute or less (Automated)](#page431) [430](#page431)

[5.2.18 Ensure SSH warning banner is configured (Automated)](#page433) [432](#page433)

[5.2.19 Ensure SSH PAM is enabled (Automated)](#page434) [433](#page434)

[5.2.20 Ensure SSH AllowTcpForwarding is disabled (Automated)](#page436) [435](#page436)

[5.2.21 Ensure SSH MaxStartups is configured (Automated)](#page438) [437](#page438)

[5.2.22 Ensure SSH MaxSessions is limited (Automated)](#page439) [438](#page439)

[5.3 Configure PAM](#page440) [439](#page440)

[5.3.1 Ensure password creation requirements are configured (Automated)](#page441) [440](#page441)

[5.3.2 Ensure lockout for failed password attempts is configured (Automated) .. 443](#page444)

[5.3.3 Ensure password reuse is limited (Automated)](#page447) [446](#page447)

[5.4 User Accounts and Environment](#page449) [448](#page449)

[5.4.1 Set Shadow Password Suite Parameters](#page450) [449](#page450)

[5.4.1.1 Ensure password hashing algorithm is SHA-512 (Automated)](#page451) [450](#page451)

[5.4.1.2 Ensure password expiration is 365 days or less (Automated)](#page453) [452](#page453)

[5.4.1.3 Ensure minimum days between password changes is configured](#page455)

[(Automated)](#page455) [454](#page455)

[5.4.1.4 Ensure password expiration warning days is 7 or more (Automated)](#page457) [456](#page457)

[5.4.1.5 Ensure inactive password lock is 30 days or less (Automated)](#page459) [458](#page459)

[5.4.1.6 Ensure all users last password change date is in the past (Automated) .. 460](#page461)

[5.4.2 Ensure system accounts are secured (Automated)](#page462) [461](#page462)

[5.4.3 Ensure default group for the root account is GID 0 (Automated)](#page464) [463](#page464)

[5.4.4 Ensure default user shell timeout is configured (Automated)](#page465) [464](#page465)

[5.4.5 Ensure default user umask is configured (Automated)](#page468) [467](#page468)

[5.5 Ensure root login is restricted to system console (Manual)](#page472) [471](#page472)

[5.6 Ensure access to the su command is restricted (Automated)](#page473) [472](#page473)

[6 System Maintenance](#page475) [474](#page475)

[6.1 System File Permissions](#page476) [475](#page476)

[6.1.1 Audit system file permissions (Manual)](#page477) [476](#page477)

[6.1.2 Ensure permissions on /etc/passwd are configured (Automated)](#page480) [479](#page480)



9 | P a g e

[6.1.3 Ensure permissions on /etc/shadow are configured (Automated)](#page481) [480](#page481)

[6.1.4 Ensure permissions on /etc/group are configured (Automated)](#page482) [481](#page482)

[6.1.5 Ensure permissions on /etc/passwd- are configured (Automated)](#page483) [482](#page483)

[6.1.6 Ensure permissions on /etc/shadow- are configured (Automated)](#page484) [483](#page484)

[6.1.7 Ensure permissions on /etc/group- are configured (Automated)](#page485) [484](#page485)

[6.1.8 Ensure no world writable files exist (Automated)](#page486) [485](#page486)

[6.1.9 Ensure no unowned files or directories exist (Automated)](#page488) [487](#page488)

[6.1.10 Ensure no ungrouped files or directories exist (Automated)](#page490) [489](#page490)

[6.1.11 Audit SUID executables (Manual)](#page492) [491](#page492)

[6.1.12 Audit SGID executables (Manual)](#page494) [493](#page494)

[6.2 User and Group Settings](#page496) [495](#page496)

[6.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated) . 496](#page497)

[6.2.2 Ensure /etc/shadow password fields are not empty (Automated)](#page499) [498](#page499)

[6.2.3 Ensure root is the only UID 0 account (Automated)](#page500) [499](#page500)

[6.2.4 Ensure root PATH Integrity (Automated)](#page501) [500](#page501)

[6.2.5 Ensure all users' home directories exist (Automated)](#page503) [502](#page503)

[6.2.6 Ensure users' home directories permissions are 750 or more restrictive](#page505)

[(Automated)](#page505) [504](#page505)

[6.2.7 Ensure users own their home directories (Automated)](#page507) [506](#page507)

[6.2.8 Ensure users' dot files are not group or world writable (Automated)](#page509) [508](#page509)

[6.2.9 Ensure no users have .forward files (Automated)](#page511) [510](#page511)

[6.2.10 Ensure no users have .netrc files (Automated)](#page513) [512](#page513)

[6.2.11 Ensure users' .netrc Files are not group or world accessible (Automated)](#page515)

[514](#page515)

[6.2.12 Ensure no users have .rhosts files (Automated)](#page518) [517](#page518)

[6.2.13 Ensure all groups in /etc/passwd exist in /etc/group (Automated)](#page520) [519](#page520)

[6.2.14 Ensure no duplicate UIDs exist (Automated)](#page521) [520](#page521)

[6.2.15 Ensure no duplicate GIDs exist (Automated)](#page522) [521](#page522)

[6.2.16 Ensure no duplicate user names exist (Automated)](#page523) [522](#page523)

[6.2.17 Ensure no duplicate group names exist (Automated)](#page524) [523](#page524)

[6.2.18 Ensure shadow group is empty (Automated)](#page525) [524](#page525)

[Appendix: Recommendation Summary Table](#page526) [525](#page526)

[Appendix: CIS Controls v7 IG 1 Mapped Recommendations](#page535) [534](#page535)

[Appendix: CIS Controls v7 IG 2 Mapped Recommendations](#page540) [539](#page540)

[Appendix: CIS Controls v7 IG 3 Mapped Recommendations](#page546) [545](#page546)



10 | P a g e

[Appendix: CIS Controls v8 IG 1 Mapped Recommendations](#page552) [551](#page552)

[Appendix: CIS Controls v8 IG 2 Mapped Recommendations](#page557) [556](#page557)

[Appendix: CIS Controls v8 IG 3 Mapped Recommendations](#page564) [563](#page564)

[Appendix: Change History](#page571) [570](#page571)



11 | P a g e

**Overview**

This document provides prescriptive guidance for establishing a secure configuration posture for SUSE Linux Enterprise 15 systems running on x86 or x64 platforms. This document was tested against SUSE Linux Enterprise Server 15 SP3.

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

To obtain the latest version of this guide, please visit the [CIS SUSE Linux Enterprise Server](https://workbench.cisecurity.org/communities/15) [community](https://workbench.cisecurity.org/communities/15) . If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org

**Intended Audience**

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate SUSE Linux Enterprise 15 on a x86 or x64 platform.

**Consensus Guidance**

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

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



12 | P a g e

**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. | |  |
| *<italic font in brackets>* | | | | Italic texts set in angle brackets denote a variable | |  |
|  |  |  |  | requiring substitution for a real value. | |  |
| *Italic font* | | | | Used to denote the title of a book, article, or other | |  |
|  |  |  |  | publication. | |  |
| **Note** | | | | Additional information or caveats | |  |

**Assessment Status**

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

**Automated**

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

**Manual**

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



13 | P a g e

**Profile Definitions**

The following configuration profiles are defined by this Benchmark:

* **Level 1 - Server**

Items in this profile intend to:

1. be practical and prudent;
2. provide a clear security benefit; and
   1. 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:

* 1. are intended for environments or use cases where security is paramount.

1. acts as defense in depth measure.
   1. 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:
  1. be practical and prudent;

1. provide a clear security benefit; and
   1. 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:

* 1. are intended for environments or use cases where security is paramount.

1. acts as defense in depth measure.
2. may negatively inhibit the utility or performance of the technology. This profile is intended for workstations.



14 | P a g e

**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**

Anurag Pal

Bill Erickson

Bradley Hieber

Dave Billing

Dominic Pace

Edward Byrd

Ely Pinto

Fredrik Silverskär

James Trigg

Joy Latten

Kenneth Karlsson

Kirill Antonenko

Koen Laevens

Mark Birch

Martynas Brijunas

Mike D. Cross

Rael Daruszka

Stefan Evans

Thomas Sjögren

**Editor**

Jonathan Lewis Christopherson

Eric Pinnell

Justin Brown



15 | P a g e

**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.



16 | P a g e

***1.1 Filesystem Configuration***

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

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

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



17 | P a g e

***1.1.1 Disable unused filesystems***

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

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

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



18 | P a g e

*1.1.1.1 Ensure mounting of squashfs filesystems is disabled (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

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

**Rationale:**

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

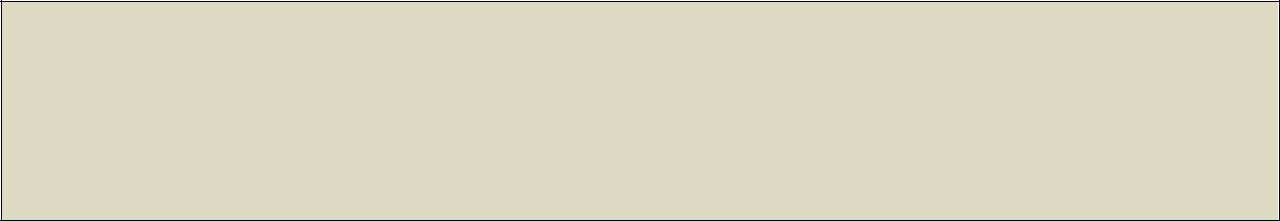
**Impact:**

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

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

**Audit:**

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



* modprobe -n -v squashfs | grep -E '(squashfs|install)' install /bin/true
* lsmod | grep squashfs

<No output>



19 | P a g e

**Remediation:**

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

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

and add the following line:



install squashfs /bin/true

Run the following command to unload the squashfs module:



# modprobe -r squashfs

**CIS Controls:**

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



20 | P a g e

*1.1.1.2 Ensure mounting of udf filesystems is disabled (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

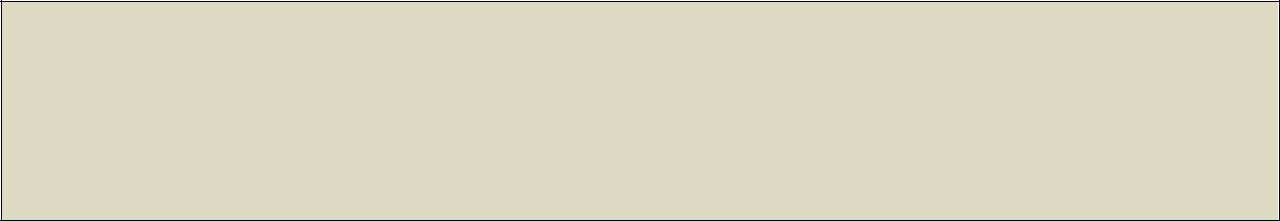
The udf filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats.

**Rationale:**

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

**Audit:**

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



* modprobe -n -v udf | grep -E '(udf|install)' install /bin/true
* lsmod | grep udf

<No output>

**Remediation:**

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

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

and add the following line:



install udf /bin/true

Run the following command to unload the udf module:



# modprobe -r udf



21 | P a g e

**CIS Controls:**

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



22 | P a g e

*1.1.1.3 Ensure mounting of FAT filesystems is limited (Automated)*

**Profile Applicability:**

* Level 2 - Workstation
* Level 2 - Server

**Description:**

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

**Rationale:**

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

*Notes:*

* *The FAT filesystem format is used by UEFI systems for the EFI boot partition. Disabling the vfat module can prevent boot on UEFI systems.*
* *FAT filesystems are often used on portable USB sticks and other flash media which are commonly used to transfer files between workstations, removing VFAT support may prevent the ability to transfer files in this way.*

**Impact:**

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

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



23 | P a g e

**Audit:**

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

Run the following command



grep -E -i '\svfat\s' /etc/fstab

And review that any output is appropriate for your environment

If not utilizing UEFI

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



* modprobe -n -v fat | grep -E '(fat|install)' install /bin/true
* lsmod | grep fat

<No output>

* modprobe -n -v vfat | grep -E '(vfat|install)' install /bin/true
* lsmod | grep vfat

<No output>

* modprobe -n -v msdos | grep -E '(msdos|install)' install /bin/true
* lsmod | grep msdos

<No output>



24 | P a g e

**Remediation:**

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf and add the following lines:

*Example: vim /etc/modprobe.d/fat.conf*



install fat /bin/true

install vfat /bin/true

install msdos /bin/true

Run the following commands to unload the msdos, vfat, and fat modules:



* modprobe -r msdos
* modprobe -r vfat
* modprobe -r fat

**CIS Controls:**

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



25 | P a g e

*1.1.2 Ensure /tmp is configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

*Notes:*

* *If an entry for /tmp exists in /etc/fstab it will take precedence over entries in the tmp.mount file.*
* *tmpfs can be resized using the size={size} parameter in /etc/fstab or on the Options line in the tmp.mount file. If we don't specify the size, it will be half the RAM.*

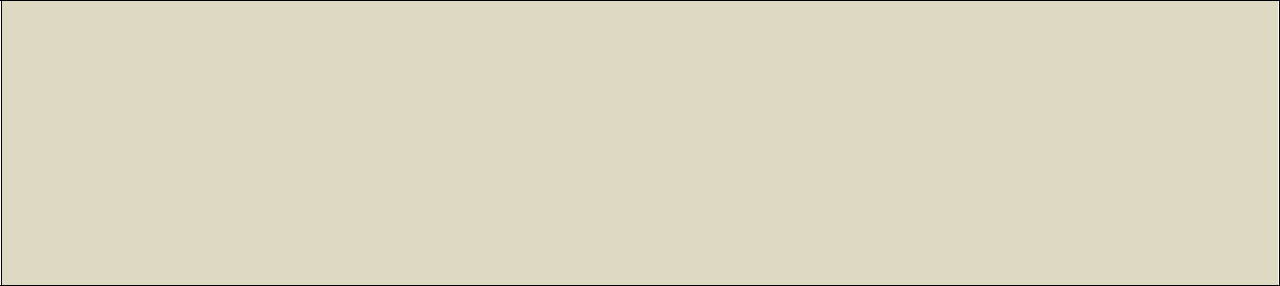
*Resize tmpfs examples:*

* */etc/fstab*



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

* *tmp.mount*



[Mount]

What=tmpfs

Where=/tmp

Type=tmpfs

Options=mode=1777,strictatime,size=2G,noexec,nodev,nosuid

**Rationale:**

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

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



26 | P a g e

**Impact:**

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

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

**Audit:**

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



# mount | grep -E '\s/tmp\s'

tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)

*If /etc/fstab is used:*

* + Run the following command and verify that tmpfs has been mounted to, or a system partition has been created for /tmp
* grep -E '\s/tmp\s' /etc/fstab | grep -E -v '^\s\*#'



tmpfs /tmp tmpfs defaults,noexec,nosuid,nodev 0 0

*OR*

*If systemd tmp.mount file is used:*

• Run the following command and verify that tmp.mount is enabled:

* systemctl is-enabled tmp.mount



enabled



27 | P a g e

**Remediation:**

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

*If /etc/fstab is used:*

* Configure /etc/fstab as appropriate.



Example:

tmpfs /tmp

tmpfs

defaults,rw,nosuid,nodev,noexec,relatime 0 0

* + Run the following command to remount /tmp
* mount -o remount,noexec,nodev,nosuid /tmp



*OR*

*If an explicit systemd target is used to mount /tmp:*

* + Run the following command to create the file /etc/systemd/system/tmp.mount if it doesn't exist:
* [ ! -f /etc/systemd/system/tmp.mount ] && cp -v /usr/share/systemd/tmp.mount /etc/systemd/system/



28 | P a g e

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

*Example tmp.mount file:*



* This file is part of systemd.
* systemd is free software; you can redistribute it and/or modify it
* under the terms of the GNU Lesser General Public License as published by
* the Free Software Foundation; either version 2.1 of the License, or
* (at your option) any later version.

[Unit]

Description=Temporary Directory (/tmp)

Documentation=man:hier(7)

Documentation=https://www.freedesktop.org/wiki/Software/systemd/APIFileSystem

s

ConditionPathIsSymbolicLink=!/tmp

DefaultDependencies=no

Conflicts=umount.target

Before=local-fs.target umount.target

After=swap.target

[Mount]

What=tmpfs

Where=/tmp

Type=tmpfs

Options=mode=1777,strictatime,nosuid,nodev,nosuid

[Install]

WantedBy=local-fs.target

* + Run the following command to reload the systemd daemon:
* systemctl daemon-reload
  + Run the following command to unmask tmp.mount:
* systemctl unmask tmp.mount
  + Run the following command to enable and start tmp.mount:
* systemctl enable --now tmp.mount



29 | P a g e

**References:**

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

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| Data Protection | | | | | |  |  |  |  |
|  |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | | |  |  |  |  |
|  |  | |  | | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | | |  |  |  |  |



30 | P a g e

*1.1.3 Ensure noexec option set on /tmp partition (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

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

Run the following command and verify that nothing is returned:



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



31 | P a g e

**Remediation:**

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

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

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



# mount -o remount,noexec /tmp

*OR*

*If an explicit systemd target is used to mount /tmp:*

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

mount options:



[Mount]

Options=mode=1777,strictatime,noexec,nodev,nosuid

Run the following command to restart the systemd daemon:



* systemctl daemon-reload

Run the following command to restart tmp.mount



# systemctl restart tmp.mount

**Additional Information:**

These remediation steps are based on following the remediation guidance in item 1.1.2. If a different file name was used that name should replace tmp.mount in the path

/etc/systemd/system/local-fs.target.wants/tmp.mount

The contents of /etc/systemd/system/local-fs.target.wants should exist as a symlink

to the file created in /etc/systemd/system.

If the path /etc/systemd/system/local-fs.target.wants/tmp.mount does not exist this

could indicate that the remediation steps from 1.1.2 were not completed successfully.



32 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a 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 | 2.6 Address unapproved software | | | | ● | ● | ● |  |
|  |  |  | |  |
| Ensure that unauthorized software is either removed or the inventory is updated | | | |  |
|  | in a timely manner | | | |  |  |  |  |



33 | P a g e

*1.1.4 Ensure nodev option set on /tmp partition (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

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

Run the following command and verify that nothing is returned:



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



34 | P a g e

**Remediation:**

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

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

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



# mount -o remount,nodev /tmp

*OR*

*If an explicit systemd target is used to mount /tmp:*

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

mount options:



[Mount]

Options=mode=1777,strictatime,noexec,nodev,nosuid

Run the following command to restart the systemd daemon:



* systemctl daemon-reload

Run the following command to restart tmp.mount



# systemctl restart tmp.mount

**Additional Information:**

These remediation steps are based on following the remediation guidance in item 1.1.2. If a different file name was used that name should replace tmp.mount in the path

/etc/systemd/system/local-fs.target.wants/tmp.mount

The contents of /etc/systemd/system/local-fs.target.wants should exist as a symlink

to the file created in /etc/systemd/system.

If the path /etc/systemd/system/local-fs.target.wants/tmp.mount does not exist this

could indicate that the remediation steps from 1.1.2 were not completed successfully.



35 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | ● | ● | ● |  |
|  |  |  | |  |
| Maintain documented, standard security configuration standards for all | | | |  |
|  | authorized operating systems and software. | | | |  |  |  |  |



36 | P a g e

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

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

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

Run the following command and verify that nothing is returned:



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



37 | P a g e

**Remediation:**

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

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



# mount -o remount,nosuid /tmp

*OR*

*If an explicit systemd target is used to mount /tmp:*

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

mount options:



[Mount]

Options=mode=1777,strictatime,noexec,nodev,nosuid

Run the following command to restart the systemd daemon:



* systemctl daemon-reload

Run the following command to restart tmp.mount:



# systemctl restart tmp.mount

**Additional Information:**

These remediation steps are based on following the remediation guidance in item 1.1.2. If a different file name was used that name should replace tmp.mount in the path

/etc/systemd/system/local-fs.target.wants/tmp.mount

The contents of /etc/systemd/system/local-fs.target.wants should exist as a symlink

to the file created in /etc/systemd/system.

If the path /etc/systemd/system/local-fs.target.wants/tmp.mount does not exist this

could indicate that the remediation steps from 1.1.2 were not completed successfully.



38 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Maintain documented, standard security configuration standards for all | | | | |  |
|  | authorized operating systems and software. | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



39 | P a g e

*1.1.6 Ensure /dev/shm is configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

/dev/shm is a traditional shared memory concept. One program will create a memory portion, which other processes (if permitted) can access. If /dev/shm is not configured, tmpfs will be mounted to /dev/shm by systemd.

*Notes:*

* *An entry for /dev/shm in /etc/fstab will take precedence.*
* *tmpfs can be resized using the size={size} parameter in /etc/fstab. If we don't specify the size, it will be half the RAM.*

*Resize tmpfs example:*



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

**Rationale:**

Any user can upload and execute files inside the /dev/shm similar to the /tmp partition. Configuring /dev/shm allows an administrator to set the noexec option on the mount, making /dev/shm useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system setuid program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.



40 | P a g e

**Audit:**

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



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

tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,noexec)

Run the following command and verify an entry for /dev/shm exists in /etc/fstab:



# grep -E '\s/dev/shm\s' /etc/fstab

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

**Remediation:**

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



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

Run the following command to remount /dev/shm:



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

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Maintain documented, standard security configuration standards for all | | | | |  |
|  | authorized operating systems and software. | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



41 | P a g e

*1.1.7 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.

*Note: /dev/shm is mounted automatically by systemd. /dev/shm needs to be added to /etc/fstab to add mount options even though it is already being mounted on boot.*

**Rationale:**

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

**Audit:**

Run the following command to verify that the noexec option is set:



* mount | grep -E '\s/dev/shm\s' | grep -v noexec Nothing should be returned

**Remediation:**

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

Run the following command to remount /dev/shm:



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



42 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a 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 | 2.6 Address unapproved software | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Ensure that unauthorized software is either removed or the inventory is updated | | | | |  |
|  | in a timely manner | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



43 | P a g e

*1.1.8 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.

*Note: /dev/shm is mounted automatically by systemd. /dev/shm needs to be added to /etc/fstab to add mount options even though it is already being mounted on boot.*

**Rationale:**

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

**Audit:**

Run the following command to verify that the nodev option is set:



* mount | grep -E '\s/dev/shm\s' | grep -v nodev Nothing should be returned

**Remediation:**

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

Run the following command to remount /dev/shm:



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



44 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Maintain documented, standard security configuration standards for all | | | | |  |
|  | authorized operating systems and software. | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



45 | P a g e

*1.1.9 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.

*Note: /dev/shm is mounted automatically by systemd. /dev/shm needs to be added to /etc/fstab to add mount options even though it is already being mounted on boot.*

**Rationale:**

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

**Audit:**

Run the following command to verify that the nosuid option is set:



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

**Remediation:**

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

Run the following command to remount /dev/shm:



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



46 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Maintain documented, standard security configuration standards for all | | | | |  |
|  | authorized operating systems and software. | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



47 | P a g e

*1.1.10 Ensure separate partition exists for /var (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

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

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

**Rationale:**

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

**Impact:**

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

**Audit:**

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



# mount | grep -E '\s/var\s'

/dev/xvdg1 on /var type ext4 (rw,relatime,data=ordered)

**Remediation:**

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

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



48 | P a g e

**References:**

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

**CIS Controls:**

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



49 | P a g e

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

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

The /var/tmp directory is a world-writable directory used for temporary storage by all users and some applications and is intended for temporary files that are preserved across reboots.

*Note: tmpfs should not be used for /var/tmp/. tmpfs is a temporary filesystem that resides in memory and/or swap partition(s). Files in tmpfs are automatically cleared at each bootup.*

**Rationale:**

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

**Impact:**

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

**Audit:**

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



# mount | grep /var/tmp

<device> on /var/tmp type ext4 (rw,nosuid,nodev,noexec,relatime)



50 | P a g e

**Remediation:**

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

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

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Maintain documented, standard security configuration standards for all authorized | | | | |  |
|  | operating systems and software. | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



51 | P a g e

*1.1.12 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 /var/tmp partition exists:

Run the following command to verify that the noexec option is set:



* mount | grep -E '\s/var/tmp\s' | grep -v noexec Nothing should be returned

**Remediation:**

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

Run the following command to remount /var/tmp :



# mount -o remount,noexec /var/tmp



52 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | |  |  |  |  |
|  | Safeguard. | | | |  |  |  |  |
| v7 | 2.6 Address unapproved software | | | | ● | ● | ● |  |
|  |  |  | |  |
| Ensure that unauthorized software is either removed or the inventory is updated in | | | |  |
|  | a timely manner | | | |  |  |  |  |



53 | P a g e

*1.1.13 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 attempt to create block or character special devices in /var/tmp .

**Audit:**

If a /var/tmp partition exists:

Run the following command to verify that the nodev option is set:



* mount | grep -E '\s/var/tmp\s' | grep -v nodev Nothing should be returned

**Remediation:**

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

Run the following command to remount /var/tmp :



# mount -o remount,nodev /var/tmp



54 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Maintain documented, standard security configuration standards for all authorized | | | | |  |
|  | operating systems and software. | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



55 | P a g e

*1.1.14 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 /var/tmp partition exists:

Run the following command to verify that that the nosuid option is set:



* mount | grep -E '\s/var/tmp\s' | grep -v nosuid Nothing should be returned

**Remediation:**

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

Run the following command to remount /var/tmp :



# mount -o remount,nosuid /var/tmp



56 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Maintain documented, standard security configuration standards for all authorized | | | | |  |
|  | operating systems and software. | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



57 | P a g e

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

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

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

**Rationale:**

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

*Note: 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.*

**Impact:**

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

**Audit:**

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



# mount | grep -E '\s/var/log\s'

<device> on /var/log type ext4 (rw,nosuid,nodev,noexec,relatime)

**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.



58 | P a g e

**References:**

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

**CIS Controls:**

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



59 | P a g e

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

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

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

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

**Rationale:**

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

**Impact:**

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

**Audit:**

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



# mount | grep /var/log/audit

/dev/xvdi1 on /var/log/audit type ext4 (rw,relatime,data=ordered)

**Remediation:**

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

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



60 | P a g e

**References:**

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

**CIS Controls:**

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



61 | P a g e

*1.1.17 Ensure separate partition exists for /home (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

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

**Rationale:**

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

**Impact:**

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

**Audit:**

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



# mount | grep /home

/dev/xvdf1 on /home type ext4 (rw,nodev,relatime,data=ordered)

**Remediation:**

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

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

**References:**

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



62 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Maintain documented, standard security configuration standards for all authorized | | | | |  |
|  | operating systems and software. | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



63 | P a g e

*1.1.18 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.

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

**Rationale:**

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

**Audit:**

If a /home partition exists:

Run the following command to verify that that the nodev option is set:



* mount | grep -E '\s/home\s' | grep -v nodev Nothing should be returned

**Remediation:**

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

Run the following command to remount /home/ with the nodev mount option:



# mount -o remount,nodev /home



64 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Maintain documented, standard security configuration standards for all authorized | | | | |  |
|  | operating systems and software. | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



65 | P a g e

*1.1.19 Ensure noexec option set on removable media partitions (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

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



# mount

**Remediation:**

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



66 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 2.6 Address unapproved software | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Ensure that unauthorized software is either removed or the inventory is updated in | | | | |  |
|  | a timely manner | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



67 | P a g e

*1.1.20 Ensure nodev option set on removable media partitions (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

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



# mount

**Remediation:**

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

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Maintain documented, standard security configuration standards for all authorized | | | | |  |
|  | operating systems and software. | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



68 | P a g e

*1.1.21 Ensure nosuid option set on removable media partitions (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

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



# mount

**Remediation:**

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

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Maintain documented, standard security configuration standards for all authorized | | | | |  |
|  | operating systems and software. | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



69 | P a g e

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

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

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



* df --local -P 2> /dev/null | 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 '{}'



70 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data access | | | | | | ● | ● | ● |  |
| control lists, also known as access permissions, to local and remote file systems, | | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | | |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | | |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | | |  |  |  |  |
|  | Safeguard. | | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | | ● | ● | ● |  |
|  |  |  |  | | |  |
| Maintain documented, standard security configuration standards for all authorized | | | | | |  |
|  | operating systems and software. | | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| Data Protection | | | | | |  |  |  |  |
|  |  |  |  |  |



71 | P a g e

*1.1.23 Disable Automounting (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 2 - Workstation

**Description:**

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

*Notes:*

* *Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.*
* *This control should align with the tolerance of the use of portable drives and optical media in the organization.*

o *On a server requiring an admin to manually mount media can be part of defense-in-depth to reduce the risk of unapproved software or information being introduced or proprietary software or information being exfiltrated.*

o *If admins commonly use flash drives and Server access has sufficient physical controls, requiring manual mounting may not increase security.*

**Rationale:**

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

**Impact:**

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

**Audit:**

Run the following command to verify autofs is not enabled:



# systemctl is-enabled autofs

Verify result is not enabled.



72 | P a g e

**Remediation:**

Run the following command to mask autofs:



# systemctl --now mask autofs

**CIS Controls:**

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



73 | P a g e

***1.2 Configure Software Updates***

Most distributions use a package manager such as yum, apt, or zypper to install and update software packages. Patch management procedures may vary widely between enterprises. Large enterprises may choose to install a local updates server that can be used in place of their distributions servers, whereas a single deployment of a system may prefer to get updates directly. Updates can be performed automatically or manually, depending on the site's policy for patch management. Many large enterprises prefer to test patches on a non-production system before rolling out to production.

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



74 | P a g e

*1.2.1 Ensure GPG keys are configured (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

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



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

**Remediation:**

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

**CIS Controls:**

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



75 | P a g e

*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 to verify repositories are configured correctly:



# zypper repos

**Remediation:**

Configure your package manager repositories according to site policy.

**CIS Controls:**

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



76 | P a g e

# grep ^\s\*gpgcheck /etc/zypp/zypp.conf gpgcheck=1

Run the following command and verify that all instances of

Run the following command and verify

gpgcheck is set to 1:

*1.2.3 Ensure gpgcheck is globally activated (Automated)*

***Profile Applicability:***

***• Level 1 - Server***

***• Level 1 - Workstation***

***Description:***

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

***Rationale:***

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

***Audit:***

******

gpgcheck returned are set to 1:

******

* awk -v 'RS=[' -F '\n' '/\n\s\*enabled\s\*=\s\*1(\W.\*)?$/ && ! /\n\s\*gpgcheck\s\*=\s\*1(\W.\*)?$/ { t=substr($1, 1, index($1, "]")-1); print t, "does not have gpgcheck enabled." }' /etc/zypp/repos.d/\*.repo

**Remediation:**

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

Edit any failing files in /etc/zypp/repos.d/\*.repo and set all instances of gpgcheck to 1.

******

77 | P a g e

**CIS Controls:**

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



78 | P a g e

***1.3 Configure sudo***

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

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



79 | P a g e

*1.3.1 Ensure sudo is installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

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

**Audit:**

Run the following command to verify that sudo is installed:



* rpm -q sudo sudo-<VERSION>

**Remediation:**

Run the following command to install sudo.



# zypper install sudo

**References:**

1. SUDO(8)



80 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | Establish and maintain a secure configuration process for enterprise assets (end- | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 4 Controlled Use of Administrative Privileges | | | | |  |  |  |  |
|  | Controlled Use of Administrative Privileges | |  | |  |  |  |  |
|  |  |  |  |  |  |



81 | P a g e

TO FILE>

*1.3.2 Ensure sudo commands use pty (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

*Note: visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the sudoers file is currently being edited you will receive a message to try again later. The -f option allows you to tell visudo which file to edit.*

**Rationale:**

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

This can be mitigated by configuring sudo to run other commands only from a pseudo-pty, whether I/O logging is turned on or not.

**Audit:**

Run the following command to verify that sudo can only run other commands from a pseudo-pty:



* grep -Ei '^\s\*Defaults\s+([^#]\S+,\s\*)?use\_pty\b' /etc/sudoers /etc/sudoers.d/\*

Defaults use\_pty

**Remediation:**

Edit the file /etc/sudoers or a file in /etc/sudoers.d/ with visudo or visudo -f <PATH

and add the following line:



Defaults use\_pty

**References:**

1. SUDO(8)



82 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | Establish and maintain a secure configuration process for enterprise assets (end- | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 4 Controlled Use of Administrative Privileges | | | | |  |  |  |  |
|  | Controlled Use of Administrative Privileges | |  | |  |  |  |  |
|  |  |  |  |  |  |



83 | P a g e

*1.3.3 Ensure sudo log file exists (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

sudo can use a custom log file

*Note: visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the sudoers file is currently being edited you will receive a message to try again later. The -f option allows you to tell visudo which file to edit.*

**Rationale:**

A sudo log file simplifies auditing of sudo commands

**Impact:**

Editing the sudo configuration incorrectly can cause sudo to stop functioning

**Audit:**

Verify that sudo has a custom log file configured

Run the following command:



* grep -Ei '^\s\*Defaults\s+([^#;]+,\s\*)?logfile\s\*=\s\*(")?[^#;]+(")?' /etc/sudoers /etc/sudoers.d/\*

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

**Remediation:**

edit the file /etc/sudoers or a file in /etc/sudoers.d/ with visudo or visudo -f <PATH

TO FILE> and add the following line:



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

**Example**



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



84 | P a g e

**References:**

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

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 8.5 Collect Detailed Audit Logs | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | 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. | | | |  |  |  |  |
|  | 6.3 Enable Detailed Logging | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | Enable system logging to include detailed information such as an event source, | | | |  | ● | ● |  |
| date, user, timestamp, source addresses, destination addresses, and other useful | | | |  |  |
|  |  |  |  |  |
|  | elements. | | | |  |  |  |  |



85 | P a g e

***1.4 Filesystem Integrity Checking***

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



86 | P a g e

*1.4.1 Ensure AIDE is installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

*Note: 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.*

**Rationale:**

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

**Audit:**

Run the following command and verify aide is installed:



* rpm -q aide aide-<version>

**Remediation:**

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

Run the following command to install AIDE:



# zypper install aide

Run the following commands to initialize AIDE:



* aide --init
* mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db



87 | P a g e

**CIS Controls:**

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



88 | P a g e

*1.4.2 Ensure filesystem integrity is regularly checked (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

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

**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 determine if there is a cron job scheduled to run the aide check.



* crontab -u root -l | grep aide
* grep -r aide /etc/cron.\* /etc/crontab

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



89 | P a g e

**Remediation:**

*If cron will be used to schedule and run aide check*

Run the following command:



# crontab -u root -e

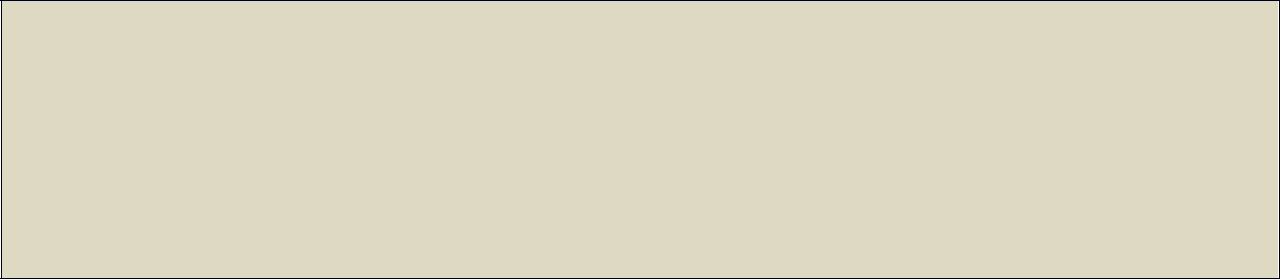
Add the following line to the crontab:



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

*OR*

*If aidecheck.service and aidecheck.timer will be used to schedule and run aide check:* Create or edit the file /etc/systemd/system/aidecheck.service and add the following lines:



[Unit]

Description=Aide Check

[Service]

Type=simple

ExecStart=/usr/sbin/aide --check

[Install]

WantedBy=multi-user.target

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



[Unit]

Description=Aide check every day at 5AM

[Timer]

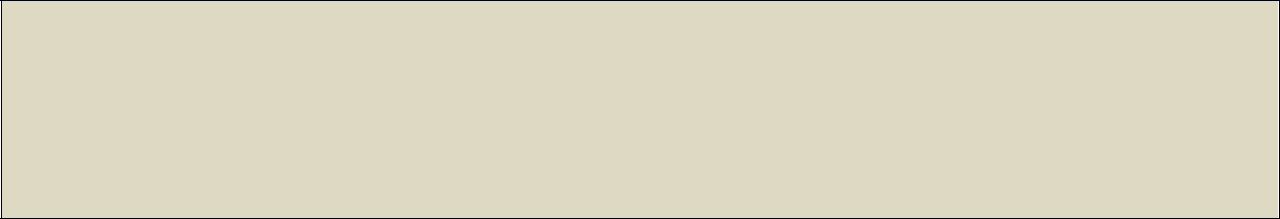
OnCalendar=\*-\*-\* 05:00:00

Unit=aidecheck.service

[Install]

WantedBy=multi-user.target

Run the following commands:



* chown root:root /etc/systemd/system/aidecheck.\*
* chmod 0644 /etc/systemd/system/aidecheck.\*
* systemctl daemon-reload
* systemctl enable aidecheck.service
* systemctl --now enable aidecheck.timer



90 | P a g e

**References:**

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

**CIS Controls:**

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



91 | P a g e

***1.5 Secure Boot Settings***

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



92 | P a g e

*1.5.1 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

*Notes:*

* *This recommendation is designed around the grub2 bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings. Replace `/boot/grub2/grub.cfg with the appropriate grub configuration file for your environment*
* *The information can be placed in any /etc/grub.d file as long as that file is incorporated into grub.cfg*

o *The superuser/user information and password should not be contained in the /etc/grub.d/00\_header file.*

o *A custom file, such as /etc/grub.d/40\_custom should be used so it is not overwritten should the Grub package be updated.*

**Rationale:**

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

**Impact:**

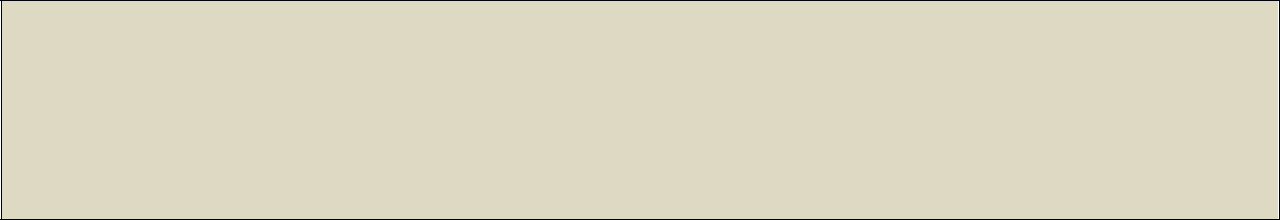
* If password protection is enabled, only the designated superuser can edit a Grub 2 menu item by pressing "e" or access the GRUB 2 command line by pressing "c"
* If GRUB 2 is set up to boot automatically to a password-protected menu entry the user has no option to back out of the password prompt to select another menu entry. Holding the SHIFT key will not display the menu in this case. The user must enter the correct username and password. If unable, the configuration files will have to be edited via the LiveCD or other means to fix the problem
* You can add --unrestricted to the menu entries to allow the system to boot without entering a password. Password will still be required to edit menu items.



93 | P a g e

**Audit:**

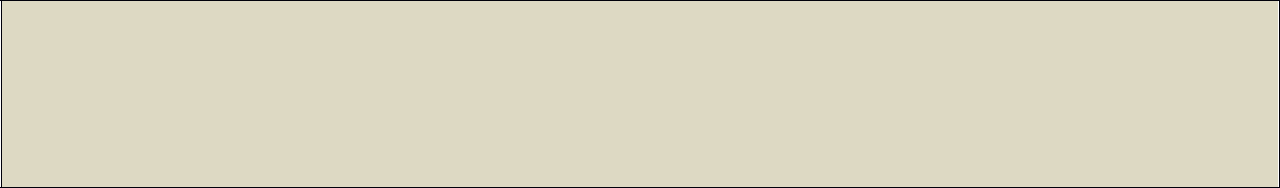
Run the following commands:



* grep "^\s\*set superusers" /boot/grub2/grub.cfg set superusers="<username>"
* grep "^\s\*password" /boot/grub2/grub.cfg password\_pbkdf2 <username> <encrypted-password>

**Remediation:**

create an encrypted password with grub2-mkpasswd-pbkdf2:



# grub2-mkpasswd-pbkdf2

Enter password: <password>

Reenter password: <password>

Your PBKDF2 is <encrypted-password>

Add the following into /etc/grub.d/40\_custom



set superusers="<username>"

password\_pbkdf2 <username> <encrypted-password>

Run the following command to update the grub2 configuration:



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

**References:**

1. <https://documentation.suse.com/sles/15-SP1/html/SLES-all/cha-grub2.html>



94 | P a g e

**CIS Controls:**

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



95 | P a g e

*1.5.2 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. The grub2 configuration is usually grub.cfg stored in

/boot/grub2/.

*Notes:*

* *This recommendation is designed around the grub2 bootloader.*
* *If LILO or another bootloader is in use in your environment:*

1. *Enact equivalent settings*
2. *Replace /boot/grub2/grub.cfg and /boot/grub2/user.cfg with the*

*appropriate boot configuration files for your environment*

**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 0/root and Access does not grant permissions to group or other :



# stat /boot/grub2/grub.cfg

Access: (0600/-rw-------) Uid: ( 0/ root) Gid: ( 0/ root)



96 | P a g e

**Remediation:**

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



* chown root:root /boot/grub2/grub.cfg
* chmod og-rwx /boot/grub2/grub.cfg

**CIS Controls:**

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



97 | P a g e

*1.5.3 Ensure authentication required for single user mode (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

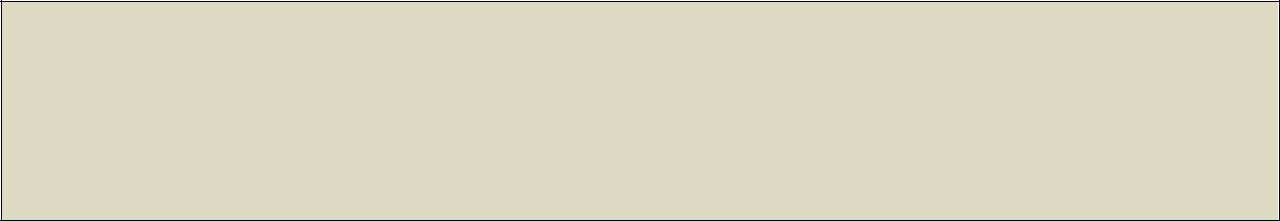
Single user mode (rescue mode) is used for recovery when the system detects an issue during boot or by manual selection from the bootloader.

**Rationale:**

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

**Audit:**

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



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

**Remediation:**

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



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

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



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



98 | P a g e

**CIS Controls:**

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



99 | P a g e

***1.6 Additional Process Hardening***



100 | P a g e

*1.6.1 Ensure core dumps are restricted (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

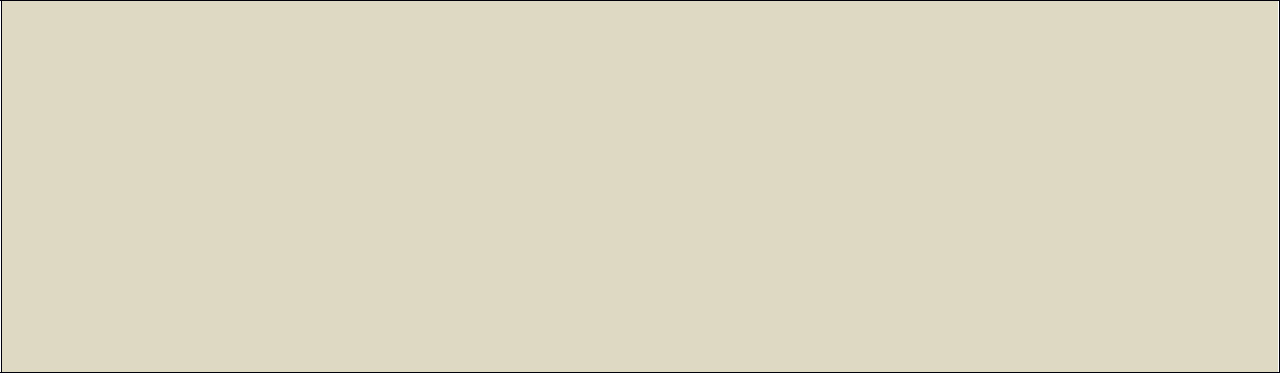
A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user.

**Rationale:**

Setting a hard limit on core dumps prevents users from overriding the soft variable. If core dumps are required, consider setting limits for user groups (see limits.conf(5) ). In addition, setting the fs.suid\_dumpable variable to 0 will prevent setuid programs from dumping core.

**Audit:**

Run the following commands and verify output matches:



* grep -E "^\s\*\\*\s+hard\s+core" /etc/security/limits.conf /etc/security/limits.d/\*

\* hard core 0

* sysctl fs.suid\_dumpable fs.suid\_dumpable = 0
* grep "fs\.suid\_dumpable" /etc/sysctl.conf /etc/sysctl.d/\* fs.suid\_dumpable = 0

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



# systemctl is-enabled coredump.service

if enabled or disabled is returned systemd-coredump is installed



101 | P a g e

**Remediation:**

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

file:



\* hard core 0

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



fs.suid\_dumpable = 0

Run the following command to set the active kernel parameter:



# sysctl -w fs.suid\_dumpable=0

If systemd-coredump is installed:

edit /etc/systemd/coredump.conf and add/modify the following lines:



Storage=none

ProcessSizeMax=0

Run the command:



systemctl daemon-reload

**CIS Controls:**

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



102 | P a g e

*1.6.2 Ensure XD/NX support is enabled (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

*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.*

**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



103 | P a g e

**Remediation:**

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

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

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

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 10.5 Enable Anti-Exploitation Features | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | 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™. | | | | | |  |  |  |  |
|  |  | 8.3 Enable Operating System Anti-Exploitation Features/ | | | | | |  |  |  |  |
|  |  |  |  | |  | |  |  |  |  |  |
| v7 |  | Deploy Anti-Exploit Technologies | | | | | |  | ● | ● |  |
|  |  | | |  | | |  |  |
|  | Enable anti-exploitation features such as Data Execution Prevention (DEP) or | | | | | |  |  |
|  |  | Address Space Layout Randomization (ASLR) that are available in an operating system | | | | | |  |  |  |  |
|  |  | or deploy appropriate toolkits that can be configured to apply protection to a broader | | | | | |  |  |  |  |
|  |  | set of applications and executables. | | | | | |  |  |  |  |



104 | P a g e

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

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

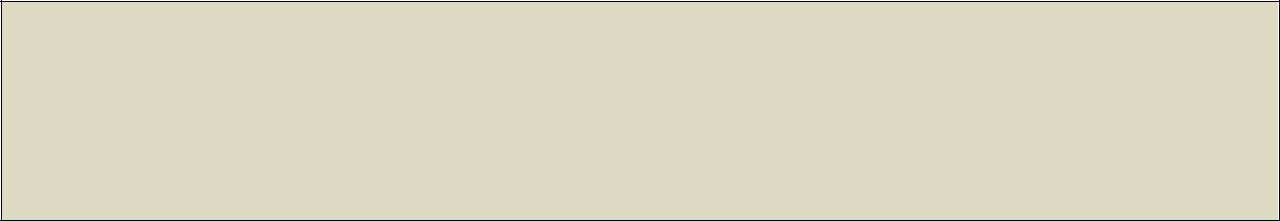
Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process.

**Rationale:**

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

**Audit:**

Run the following commands and verify output matches:



* sysctl kernel.randomize\_va\_space kernel.randomize\_va\_space = 2
* grep "kernel\.randomize\_va\_space" /etc/sysctl.conf /etc/sysctl.d/\* kernel.randomize\_va\_space = 2

**Remediation:**

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



kernel.randomize\_va\_space = 2

Run the following command to set the active kernel parameter:



# sysctl -w kernel.randomize\_va\_space=2



105 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 10.5 Enable Anti-Exploitation Features | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | 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™. | | | | | |  |  |  |  |
|  |  | 8.3 Enable Operating System Anti-Exploitation Features/ | | | | | |  |  |  |  |
|  |  |  |  | |  | |  |  |  |  |  |
| v7 |  | Deploy Anti-Exploit Technologies | | | | | |  | ● | ● |  |
|  |  | | |  | | |  |  |
|  | Enable anti-exploitation features such as Data Execution Prevention (DEP) or | | | | | |  |  |
|  |  | Address Space Layout Randomization (ASLR) that are available in an operating system | | | | | |  |  |  |  |
|  |  | or deploy appropriate toolkits that can be configured to apply protection to a broader | | | | | |  |  |  |  |
|  |  | set of applications and executables. | | | | | |  |  |  |  |



106 | P a g e

*1.6.4 Ensure prelink is disabled (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:**

Run the following command to verify that 1prelink` is not installed:



# rpm -q prelink

package prelink is not installed

**Remediation:**

Run the following command to restore binaries to normal:



# prelink -ua

Run the following command to uninstall prelink:



# zypper remove prelink



107 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.1 Establish and Maintain a Secure Configuration Process | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | | |  |  |  |  |
| v8 |  | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | | ● | ● | ● |  |
|  | and software (operating systems and applications). Review and update documentation | | | | | |  |
|  |  |  |  |  |  |
|  |  | annually, or when significant enterprise changes occur that could impact this | | | | | |  |  |  |  |
|  |  | Safeguard. | | | | | |  |  |  |  |
|  |  | 14.9 Enforce Detail Logging for Access or Changes to Sensitive | | | | | |  |  |  |  |
| v7 |  | Data | |  |  | |  |  |  | ● |  |
|  | Enforce detailed audit logging for access to sensitive data or changes to sensitive | | | | | |  |  |  |
|  |  | data (utilizing tools such as File Integrity Monitoring or Security Information and Event | | | | | |  |  |  |  |
|  |  | Monitoring). | | | | | |  |  |  |  |



108 | P a g e

***1.7 Mandatory Access Control***

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

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



109 | P a g e

***1.7.1 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:* <https://gitlab.com/apparmor/apparmor/-/wikis/Documentation>
2. *SUSE AppArmor Documentation:* <https://documentation.suse.com/sles/15-SP1/html/SLES-all/cha-apparmor-start.html>



110 | P a g e

*1.7.1.1 Ensure AppArmor is installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

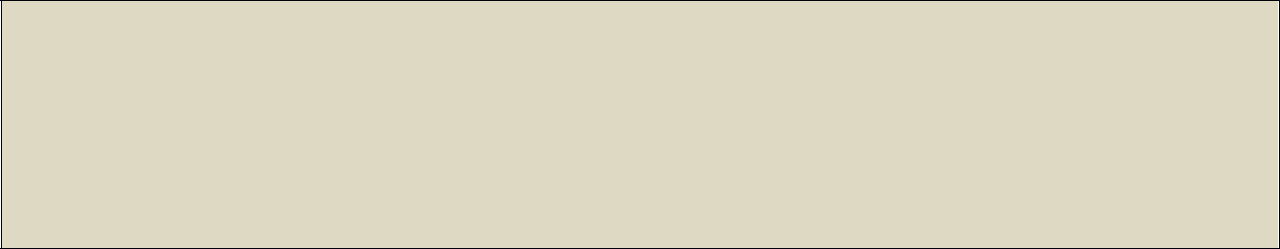
AppArmor provides Mandatory Access Controls.

**Rationale:**

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

**Audit:**

Run the following command to verify that the AppArmor packages are installed:



* rpm -q apparmor-docs apparmor-parser apparmor-profiles apparmor-utils libapparmor1

apparmor-docs-<version>

apparmor-parser-<version>

apparmor-profiles-<version>

apparmor-utils-<version>

libapparmor1-<version>

**Remediation:**

Run the following command to install AppArmor:



# zypper install -t pattern apparmor

**Default Value:**

AppArmor is installed on SLES 15 SP1 by default



111 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



112 | P a g e

*1.7.1.2 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 grub2 bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.*

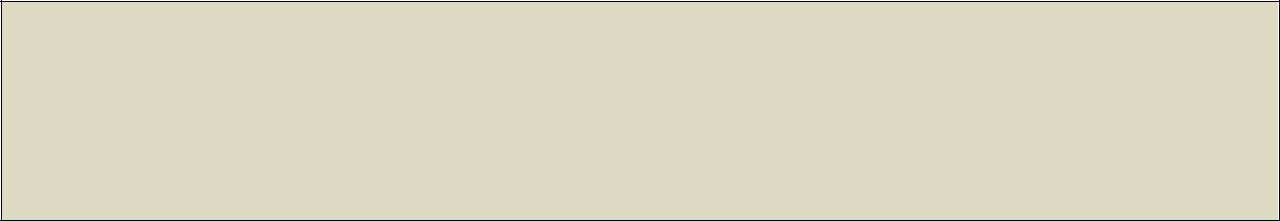
**Rationale:**

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/grub2/grub.cfg | grep -v "apparmor=1" Nothing should be returned
* grep "^\s\*linux" /boot/grub2/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:



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



113 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



114 | P a g e

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

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

AppArmor profiles define what resources applications are able to access.

**Rationale:**

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

**Audit:**

Run the following command and verify that profiles are loaded, profiles are in enforce or complain mode, and no processes are unconfined:



# 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 that 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.



115 | P a g e

**Remediation:**

Run one of the following commands to set all profiles to either enforce *OR* complain mode

* Run the following command to set all profiles to enforce mode:
  + aa-enforce /etc/apparmor.d/\*
* Run the following command to set all profiles to complain mode:
  + aa-complain /etc/apparmor.d/\*



Run the following command to list unconfined processes:



# aa-unconfined

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

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



116 | P a g e

*1.7.1.4 Ensure all AppArmor Profiles are enforcing (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

AppArmor profiles define what resources applications are able to access.

**Rationale:**

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

**Audit:**

Run the following command and verify that profiles are loaded, no profiles are in complain mode, and no processes are unconfined:



# apparmor\_status | grep profiles

Review output and ensure that profiles are loaded, and in enforce 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 to 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.



117 | P a g e

**Remediation:**

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



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

Run the following command to list unconfined processes:



# aa-unconfined

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

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



118 | P a g e

***1.8 Warning Banners***

Presenting a warning message prior to the normal user login may assist in the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific exploits at a system.

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

*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.*



119 | P a g e

***1.8.1 Command Line Warning Banners***

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



120 | P a g e

*1.8.1.1 Ensure message of the day is configured properly (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If mingetty(8) supports the following options, they display operating system information: \m - machine architecture \r - operating system release \s - operating system name \v - operating system version

**Rationale:**

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " uname -a " command once they have logged in.

**Audit:**

Run the following command and verify that the contents match site policy:



# cat /etc/motd

Run the following command and verify no results are returned:



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



121 | P a g e

**Remediation:**

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

*OR*

*If the motd is not used, this file can be removed.*

Run the following command to remove the motd file:



# rm /etc/motd

**CIS Controls:**

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



122 | P a g e

*1.8.1.2 Ensure local login warning banner is configured properly (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The contents of the /etc/issue file are displayed to users prior to login for local terminals. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If mingetty(8) supports the following options, they display operating system information: \m - machine architecture \r - operating system release \s - operating system name \v - operating system version - or the operating system's name

**Rationale:**

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " uname -a " command once they have logged in.

**Audit:**

Run the following command and verify that the contents match site policy:



# cat /etc/issue

Run the following command and verify no results are returned:



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

**Remediation:**

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



* echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue

**CIS Controls:**



123 | P a g e

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



124 | P a g e

*1.8.1.3 Ensure remote login warning banner is configured properly (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If mingetty(8) supports the following options, they display operating system information: \m - machine architecture \r - operating system release \s - operating system name \v - operating system version

**Rationale:**

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " uname -a " command once they have logged in.

**Audit:**

Run the following command and verify that the contents match site policy:



# cat /etc/issue.net

Run the following command and verify no results are returned:



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

**Remediation:**

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



* echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue.net



125 | P a g e

**CIS Controls:**

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



126 | P a g e

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

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

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



# stat /etc/motd

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

**Remediation:**

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



* chown root:root /etc/motd
* chmod u-x,go-wx /etc/motd

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



127 | P a g e

*1.8.1.5 Ensure permissions on /etc/issue are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

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



# stat /etc/issue

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

**Remediation:**

Run the following commands to set permissions on /etc/issue:



* chown root:root /etc/issue
* chmod u-x,go-wx /etc/issue

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



128 | P a g e

*1.8.1.6 Ensure permissions on /etc/issue.net are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

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



# stat /etc/issue.net

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

**Remediation:**

Run the following commands to set permissions on /etc/issue.net:



* chown root:root /etc/issue.net
* chmod u-x,go-wx /etc/issue.net

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



129 | P a g e

*1.9 Ensure updates, patches, and additional security software are installed (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Periodically patches are released for included software either due to security flaws or to include additional functionality.

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

**Rationale:**

Newer patches may contain security enhancements that would not be available through the latest full update. As a result, it is recommended that the latest software patches be used to take advantage of the latest functionality. As with any software installation, organizations need to determine if a given update meets their requirements and verify the compatibility and supportability of any additional software against the update revision that is selected.

**Audit:**

Run the following command and verify there are no updates or patches to install:



# zypper list-updates

**Remediation:**

Use your package manager to update all packages on the system according to site policy.

The following command will install all available updates:



# zypper update



130 | P a g e

**CIS Controls:**

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



131 | P a g e

*1.10 Ensure GDM is removed or login is configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The GNOME Display Manager (GDM) handles graphical login for GNOME based systems. Configuration of the GNOME desktop is managed with dconf. It is a hierarchically structured database or registry that allows users to modify their personal settings, and system administrators to set default or mandatory values for all users.

Global dconf configuration parameters can be set in the /etc/dconf/db/ directory. This includes the configuration for GDM or locking certain configuration options for users.

**Rationale:**

If a graphical login is not required, it should be removed to reduce the attack surface of the system.

If a graphical login is required, last logged in user display should be disabled, and a warning banner should be configured.

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

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place.

*Notes:*

* *This recommendation is based on the gdm profile. If a different profile name is used on*

*the system, update the gdm and gdm.d to <profilee\_name> and <profile\_name>.d*

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

*message and/or /etc/dconf/db/gdm.d/00-login-screen file.*

* *If a different GUI login service is in use and required on the system, consult your documentation to disable displaying the last logged on user and apply an equivalent banner.*



132 | P a g e

**Audit:**

Run the following command to verify the GDM is not installed on the system:



# rpm -q gdm

package gdm is not installed

*OR*

*If GDM is required:*

Verify that /etc/dconf/profile/gdm exists and includes the following:



user-db:user

system-db:gdm

file-db:/usr/share/gdm/greeter-dconf-defaults

Verify that a file exists in /etc/dconf/db/gdm.d/ and includes the following: *(This is*

*typically /etc/dconf/db/gdm.d/01-banner-message)*



[org/gnome/login-screen]

banner-message-enable=true

banner-message-text='<banner message>'

Verify that a file exists in /etc/dconf/db/gdm.d/ and includes the following: *(This is*

*typically /etc/dconf/db/gdm.d/00-login-screen)*



[org/gnome/login-screen]

disable-user-list=true



133 | P a g e

**Remediation:**

Run the following command to remove GDM



# zypper remove gdm

*OR*

*If GDM is required:*

Edit or create the gdm profile which contains the following lines: (This is typically

/etc/dconf/profile/gdm)



user-db:user

system-db:gdm

file-db:/usr/share/gdm/greeter-dconf-defaults

Run the following Run to display a login banner:

*Note: the directory /etc/dconf/db/gdm.d/ may need to be created*

Edit or create a gdm keyfile for machine-wide settings: *(This is typically*

*/etc/dconf/db/gdm.d/01-banner-message)*



[org/gnome/login-screen]

banner-message-enable=true

banner-message-text='<banner message>'

*Example Banner Text:* 'Authorized uses only. All activity may be monitored and reported.'

Run the following to disable the user list:

Edit or create a gdm keyfile for machine-wide settings in the directory

/etc/dconf/db/gdm.d/ and add the following: (This is typically /etc/dconf/db/gdm.d/00-login-screen)



[org/gnome/login-screen]

* Do not show the user list disable-user-list=true

Run the following command to update the system databases:



# dconf update

**References:**

1. <https://documentation.suse.com/sles/15-SP1/html/SLES-all/cha-gui-desktop.html>
2. <https://help.gnome.org/admin/system-admin-guide/stable>

**CIS Controls:**



134 | P a g e

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.1 Establish and Maintain a Secure Configuration Process | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | | | |  |  |  |  |
| v8 |  | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | | | ● | ● | ● |  |
|  | and software (operating systems and applications). Review and update documentation | | | | | | |  |
|  |  |  |  |  |  |
|  |  | annually, or when significant enterprise changes occur that could impact this | | | | | | |  |  |  |  |
|  |  | Safeguard. | | | | | | |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  | |  |  |  |  |  |
| v8 |  | Assets and Software | |  |  |  | | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such as | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | an unused file sharing service, web application module, or service function. | | | | | | |  |  |  |  |
| v7 |  | 2.6 Address unapproved software | | | | | | | ● | ● | ● |  |
|  |  |  | |  |  | | |  |
|  | Ensure that unauthorized software is either removed or the inventory is updated in | | | | | | |  |
|  |  | a timely manner | | | | | | |  |  |  |  |
| v7 |  | 5.1 Establish Secure Configurations | | | | | | | ● | ● | ● |  |
|  |  |  | | |  | | |  |
|  | Maintain documented, standard security configuration standards for all authorized | | | | | | |  |
|  |  | operating systems and software. | | | | | | |  |  |  |  |



135 | P a g e

***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.



136 | P a g e

***2.1 inetd Services***

inetd is a super-server daemon that provides internet services and passes connections to configured services. While not commonly used inetd and any unneeded inetd based services should be disabled if possible.



137 | P a g e

*2.1.1 Ensure xinetd is not installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The eXtended InterNET Daemon ( xinetd ) is an open source super daemon that replaced the original inetd daemon. The xinetd daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests.

**Rationale:**

If there are no xinetd services required, it is recommended that the package be removed to reduce the attack surface are of the system.

*Note: If an xinetd service or services are required, ensure that any xinetd service not required is stopped and disabled*

**Audit:**

Run the following command to verify xinetd is not installed:



# rpm -q xinetd

package xinetd is not installed

**Remediation:**

Run the following command to remove xinetd:



# zypper remove xinetd



138 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | | |  |  |  |  |
| v7 |  | 2.6 Address unapproved software | | | | | | | ● | ● | ● |  |
|  |  |  |  | |  | |  |  |
|  | Ensure that unauthorized software is either removed or the inventory is updated | | | | | | |  |
|  |  | in a timely manner | | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | | |  |  |  |  |
|  |  |  |  |  | | | |  |  |  |  |  |
| v7 |  | Running | |  | | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | | |  |  |  |  |



139 | P a g e

***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 the package be removed, or the service be stopped and masked to reduce the potential attack surface.



140 | P a g e

***2.2.1 Time Synchronization***

It is recommended that physical systems and virtual guests lacking direct access to the physical host's clock be configured to synchronize their time using a service such as chrony

or timesyncd.



141 | P a g e

*2.2.1.1 Ensure time synchronization is in use (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

*Notes:*

* *On systems where host based time synchronization is not available, verify that chrony is installed or systemd-timesyncd is enabled.*
* *On systems where host based time synchronization is available consult your documentation and verify that host based synchronization is in use.*
* *If another method for time synchronization is being used, this section may be skipped.*

**Rationale:**

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

**Audit:**

On systems where host based time synchronization is not available, verify chrony is installed *OR* systemd-timesyncd is enabled:

*Note: Only one time synchronization package should be installed and/or enabled*

Run the following command to verify that chrony is installed:



* rpm -q chrony chrony-<version>

*OR*

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



# systemctl is-enabled systemd-timesyncd



142 | P a g e

**Remediation:**

On systems where host based time synchronization is not available, install chrony *OR*

enable systemd-timesyncd:

Run the following command to install chrony:



# zypper install chrony

*OR*

Run the following command to enable systemd-timesyncd



# systemctl enable systemd-timesyncd

*Note: On systems where host based time synchronization is available consult your virtualization software documentation and setup host based synchronization.*

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
| v8 | 8.4 Standardize Time Synchronization | | | |  | ● | ● |  |
|  |  |  |  |  |  |
| Standardize time synchronization. Configure at least two synchronized time | | | |  |  |
|  | sources across enterprise assets, where supported. | | | |  |  |  |  |
|  | 6.1 Utilize Three Synchronized Time Sources | | | |  |  |  |  |
|  |  |  | |  |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



143 | P a g e

*2.2.1.2 Ensure systemd-timesyncd is configured (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.

The systemd-timesyncd daemon:

* Implements an SNTP client.
* Only implements a client side

1. Does not bother with the full NTP complexity
   1. Only on querys time from one remote server, synchronizing the local clock to it

* runs with minimal privileges
* saves the current clock to disk every time a new NTP sync has been acquired
  1. Uses this to correct the system clock early at bootup
  2. to make sure that time monotonically progresses on these systems, even if it is not always correct
* Requires a new system user and group "systemd-timesync" to be created on installation of systemd
* Hooked up with networkd to only operate when network connectivity is available

*Notes:*

* *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.*
* *This recommendation only applies if timesyncd is in use on the system*

**Rationale:**

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



144 | P a g e

**Audit:**

Ensure that timesyncd is enabled and started

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



* systemctl is-enabled systemd-timesyncd.service enabled

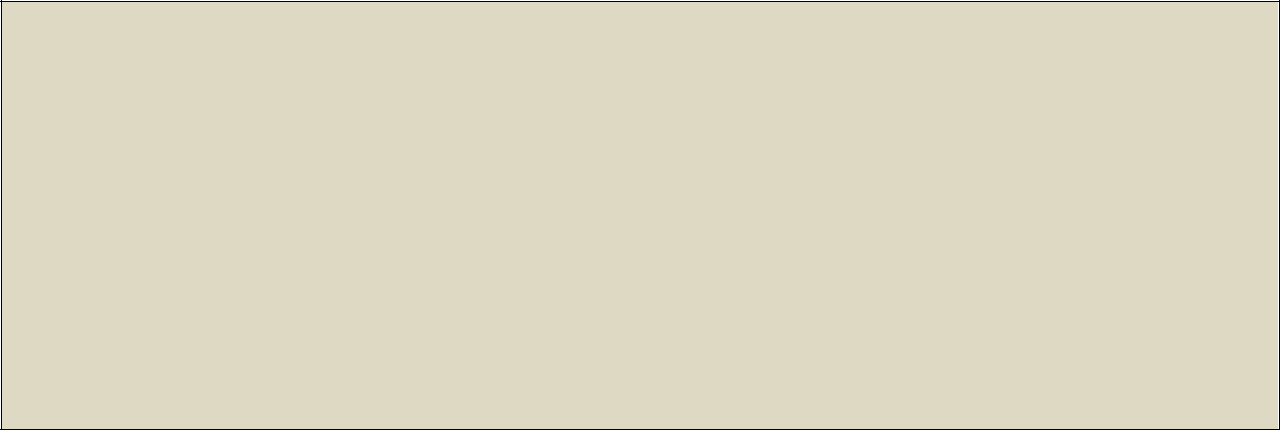
Review /etc/systemd/timesyncd.conf and ensure that the NTP servers, NTP FallbackNTP servers, and RootDistanceMaxSec listed are in accordance with local policy

Run the following command



# timedatectl status

This should return something similar to:



Local time: Tue 2019-06-04 15:40:45 EDT

Universal time: Tue 2019-06-04 19:40:45 UTC

RTC time: Tue 2019-06-04 19:40:45

Time zone: America/New\_York (EDT, -0400)

NTP enabled: yes

NTP synchronized: yes

RTC in local TZ: no

DST active: yes

Last DST change: DST began at

Sun 2019-03-10 01:59:59 EST

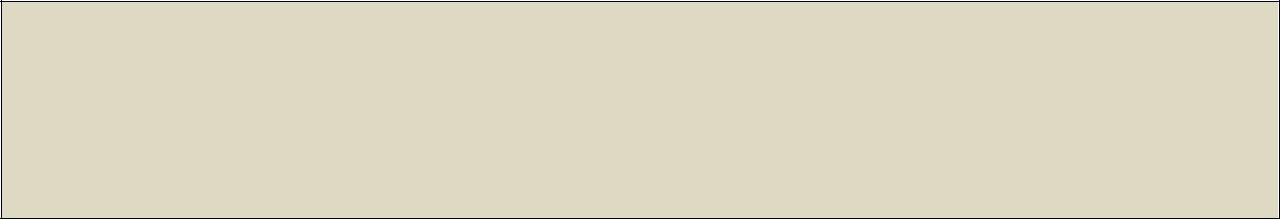
Sun 2019-03-10 03:00:00 EDT

Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2019-11-03 01:59:59 EDT

Sun 2019-11-03 01:00:00 EST

**Remediation:**

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



NTP=0.suse.pool.ntp.org 1.suse.pool.ntp.org #Servers listed should be In Accordance With Local Policy

FallbackNTP=2.suse.pool.ntp.org 3.suse.pool.ntp.org #Servers listed should be In Accordance With Local Policy

RootDistanceMax=1 #should be In Accordance With Local Policy

Run the following commands to enable and start systemd-timesyncd:



* systemctl --now enable systemd-timesyncd.service
* timedatectl set-ntp true

**CIS Controls:**



145 | P a g e

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
| v8 | 8.4 Standardize Time Synchronization | | | |  | ● | ● |  |
|  |  |  |  |  |  |
| Standardize time synchronization. Configure at least two synchronized time | | | |  |  |
|  | sources across enterprise assets, where supported. | | | |  |  |  |  |
|  | 6.1 Utilize Three Synchronized Time Sources | | | |  |  |  |  |
|  |  |  | |  |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



146 | P a g e

*2.2.1.3 Ensure chrony is configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

*Note: This recommendation only applies if chrony is in use on the system. If another method of time synchronization is in use on the system, this recommendation can be skipped.*

**Audit:**

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



* grep -E "^(server|pool)" /etc/chrony.conf server <remote-server>

Multiple servers may be configured

Run the following command and verify OPTIONS includes '-u chrony':



* grep ^OPTIONS /etc/sysconfig/chronyd OPTIONS="-u chrony"

Additional options may be present.



147 | P a g e

**Remediation:**

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



server <remote-server>

Add or edit the OPTIONS in /etc/sysconfig/chronyd to include '-u chrony':



OPTIONS="-u chrony"

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
| v8 | 8.4 Standardize Time Synchronization | | | |  | ● | ● |  |
|  |  |  |  |  |  |
| Standardize time synchronization. Configure at least two synchronized time | | | |  |  |
|  | sources across enterprise assets, where supported. | | | |  |  |  |  |
|  | 6.1 Utilize Three Synchronized Time Sources | | | |  |  |  |  |
|  |  |  | |  |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



148 | P a g e

*2.2.2 Ensure X11 Server components are not installed (Automated)*

**Profile Applicability:**

* Level 1 - Server

**Description:**

The X Window System provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Windows system is typically used on workstations where users login, but not on servers where users typically do not login.

**Rationale:**

Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.

**Impact:**

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

**Audit:**

Run the following command to Verify X Windows Server is not installed.



# rpm -qa xorg-x11-server\*

**Remediation:**

Run the following command to remove the X Windows Server packages:



# zypper remove xorg-x11-server\*

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | |  |  | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | |  |  |  |  |
| v7 |  | 2.6 Address unapproved software | | | | | ● | ● | ● |  |
|  |  |  | |  | |  |
|  | Ensure that unauthorized software is either removed or the inventory is updated | | | | |  |
|  |  | in a timely manner | | | | |  |  |  |  |



149 | P a g e

*2.2.3 Ensure Avahi Server is not installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 2 - Workstation

**Description:**

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

**Rationale:**

Automatic discovery of network services is not normally required for system functionality.

It is recommended to remove this package to reduce the potential attack surface.

**Audit:**

Run one of the following command to verify avahi-autoipd and avahi are not installed:



# rpm -q avahi-autoipd avahi

package avahi-autoipd is not installed

package avahi is not installed

**Remediation:**

Run the following commands to stop, mask and remove avahi-autoipd and avahi:



* systemctl stop avahi-daemon.socket avahi-daemon.service
* zypper remove avahi-autoipd avahi

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



150 | P a g e

*2.2.4 Ensure CUPS is not installed (Automated)*

**Profile Applicability:**

* Level 1 - Server

**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.

*Note: Removing CUPS will prevent printing from the system*

**Impact:**

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

**Audit:**

Run the following command to verify cups is not installed:



# rpm -q cups

package cups is not installed

**Remediation:**

Run the following command to remove cups:



# zypper remove cups

**References:**

1. More detailed documentation on CUPS is available at the project homepage at [http://www.cups.org.](http://www.cups.org./)



151 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



152 | P a g e

*2.2.5 Ensure DHCP Server is not installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

Run the following command to verify dhcp is not installed:



# rpm -q dhcp

package dhcp is not installed

**Remediation:**

Run the following command to remove dhcp:



# zypper remove dhcp

**References:**

1. dhcpd(8)

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



153 | P a g e

*2.2.6 Ensure LDAP server is not installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Audit:**

Run the following command to verify openldap-servers is not installed:



# rpm -q openldap2

package openldap2 is not installed

**Remediation:**

Run the following command to remove openldap-servers:



# zypper remove openldap2

**References:**

1. For more detailed documentation on OpenLDAP, go to the project homepage at [http://www.openldap.org.](http://www.openldap.org./)



154 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



155 | P a g e

nfs-kernel-server

*2.2.7 Ensure nfs-utils is not installed or the nfs-server service is masked (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 require network shares, it is recommended that the nfs-utils and

packages be removed to reduce the attack surface of the system.

*Note: many of the libvirt packages used by Enterprise Linux virtualization are dependent on the nfs-utils package. If the nfs-utils or nfs-kernel-server packages are required as a dependency, the nfs-server service should be disabled and masked to reduce the attack surface of the system*

**Audit:**

Run the following command to verify nfs-utils and nfs-kernel-server are not installed:



# rpm -q nfs-utils nfs-kernel-server

package nfs-utils is not installed

package nfs-kernel-server is not installed

*OR*

*If the nfs-utils or nfs-kernel-server packages are required as a dependency*

Run the following command to verify that the nfs-server service is masked:



* systemctl is-enabled nfs-server masked



156 | P a g e

**Remediation:**

Run the following commands to remove nfs-utils and nfs-kernel-server:



* zypper remove nfs-utils
* zypper remove nfs-kernel-server

*OR*

*If the nfs-utils or nfs-kernel-server packages are required as a dependency*

Run the following command to stop and mask the nfs-server service:



# systemctl --now mask nfs-server

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



157 | P a g e

*2.2.8 Ensure rpcbind is not installed or the rpcbind services are masked (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

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

**Rationale:**

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

*Note: many of the libvirt packages used by Enterprise Linux virtualization, and the nfs-utils package used for The Network File System (NFS) are dependent on the rpcbind package. If the rpcbind is required as a dependency, the services rpcbind.service and rpcbind.socket should be stopped and masked to reduce the attack surface of the system.*



158 | P a g e

**Audit:**

Run the following command to verify rpcbind is not installed:



# rpm -q rpcbind

package rpcbind is not installed

*OR*

*If the rpcbind packege is required as a dependency*

Run the following commands to verify that the rpcbind is masked:



* systemctl is-enabled rpcbind masked

Run the following command to verify that the rpcbind.socket is masked:



* systemctl is-enabled rpcbind.socket masked

**Remediation:**

Run the following command to remove nfs-utils:



# zypper remove rpcbind

*OR*

*If the rpcbind package is required as a dependency*

Run the following commands to stop and mask the rpcbind and rpcbind.socket services:



* systemctl --now mask rpcbind
* systemctl --now mask rpcbind.socket



159 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



160 | P a g e

*2.2.9 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 removed to reduce the potential attack surface.

**Audit:**

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



# rpm -q bind

package bind is not installed

**Remediation:**

Run the following command to remove bind:



# zypper remove bind

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



161 | P a g e

*2.2.10 Ensure FTP Server is not installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

FTP (File Transfer Protocol) is a traditional and widely used standard tool for transferring files between a server and clients over a network, especially where no authentication is necessary (permits anonymous users to connect to a server).

**Rationale:**

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

*Note: Additional FTP servers also exist and should be removed if not required.*

**Audit:**

Run the following command to verify vsftpd is not installed:



# rpm -q vsftpd

package vsftpd is not installed

**Remediation:**

Run the following command to remove vsftpd:



# zypper remove vsftpd

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



162 | P a g e

*2.2.11 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 removed to reduce the potential attack surface.

*Notes:*

* *Several http servers exist. apache, apache2, lighttpd, and nginx are example packages that provide an HTTP server*
* *These and other packages should also be audited, and removed if not required*

**Audit:**

Run the following command to verify apache2 is not installed:



# rpm -q apache2

package httpd is not installed

**Remediation:**

Run the following command to remove apache2:



# zypper remove apache2

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



163 | P a g e

*2.2.12 Ensure IMAP and POP3 server is not installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

dovecot is an open source IMAP and POP3 server for Linux based systems.

**Rationale:**

Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the package be removed to reduce the potential attack surface.

*Notes:*

* *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 and the packages removed if not required.*

**Audit:**

Run the following command to verify dovecot is not installed:



# rpm -q dovecot

package dovecot is not installed

**Remediation:**

Run the following command to remove dovecot:



# zypper remove dovecot



164 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



165 | P a g e

*2.2.13 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 package can be removed to reduce the potential attack surface.

**Audit:**

Run the following command to verify samba is not installed:



# rpm -q samba

package samba is not installed

**Remediation:**

Run the following command to remove samba:



# zypper remove samba

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



166 | P a g e

*2.2.14 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:**

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

*Note: Several HTTP proxy servers exist. These should be checked and removed unless required.*

**Audit:**

Run the following command to verify squid is not installed:



# rpm -q squid

package squid is not installed

**Remediation:**

Run the following command to remove the squid package:



# zypper remove squid

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



167 | P a g e

net-snmp

*2.2.15 Ensure net-snmp 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 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 net-snmp is not installed:



# rpm -q net-snmp

package net-snmp is not installed



168 | P a g e

**Remediation:**

Run the following command to remove net-snmpd:



# zypper remove net-snmp

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | | |  |  |  |  |
| v7 |  | 2.6 Address unapproved software | | | | | | | ● | ● | ● |  |
|  |  |  |  | |  | |  |  |
|  | Ensure that unauthorized software is either removed or the inventory is updated | | | | | | |  |
|  |  | in a timely manner | | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | | |  |  |  |  |
|  |  |  |  |  | | | |  |  |  |  |  |
| v7 |  | Running | |  | | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | | |  |  |  |  |



169 | P a g e

*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.

*Notes:*

* *This recommendation is designed around the postfix mail server.*
* *Depending on your environment you may have an alternative MTA installed such as sendmail. If this is the case consult the documentation for your installed MTA to configure the recommended state.*

**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 -E ':25\s' | grep -E -v '\s(127.0.0.1|\[?::1\]?):25\s' Nothing should be returned



170 | P a g e

**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

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



171 | P a g e

*2.2.17 Ensure rsync is not installed or the rsyncd service is masked (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

Unless required, the rsync package should be removed to reduce the attack surface area of the system.

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

*Note: If a required dependency exists for the rsync package, but the rsyncd service is not required, the service should be masked.*

**Impact:**

There are packages that are dependent on the rsync package. If the rsync package is removed, these packages will be removed as well.

Before removing the rsync package, review any dependent packages to determine if they are required on the system. If a dependent package is required, mask the rsyncd service and leave the rsync package installed.

**Audit:**

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



# rpm -q rsync

package rsync is not installed

*OR*

Run the following command to verify the rsyncd service is masked:



* systemctl is-enabled rsyncd masked

**Remediation:**



172 | P a g e

Run the following command to remove the rsync package:



# zypper remove rsync

*OR*

Run the following command to mask the rsyncd service:



# systemctl --now mask rsyncd

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



173 | P a g e

*2.2.18 Ensure NIS server is not installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The ypserv package provides the Network Information Service (NIS). This service, 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 ypserv package be removed, and if required a more secure services be used.

**Audit:**

Run the following command to verify ypserv is not installed:



# rpm -q ypserv

package ypserv is not installed

**Remediation:**

Run the following command to remove ypserv:



# zypper remove ypserv



174 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | | |  |  |  |  |
| v7 |  | 2.6 Address unapproved software | | | | | | | ● | ● | ● |  |
|  |  |  |  | |  | |  |  |
|  | Ensure that unauthorized software is either removed or the inventory is updated | | | | | | |  |
|  |  | in a timely manner | | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | | |  |  |  |  |
|  |  |  |  |  | | | |  |  |  |  |  |
| v7 |  | Running | |  | | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | | |  |  |  |  |



175 | P a g e

*2.2.19 Ensure telnet-server is not installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The telnet-server package contains the telnet daemon, which accepts connections from users from other systems via the telnet protocol.

**Rationale:**

The telnet protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow a user with access to sniff network traffic the ability to steal credentials. The ssh package provides an encrypted session and stronger security.

**Audit:**

Run the following command to verify the telnet package is not installed:



rpm -q telnet-server

package telnet-server is not installed

**Remediation:**

Run the following command to remove the telnet-server package:



# zypper remove telnet-server

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | | |  |  |  |  |
| v7 |  | 2.6 Address unapproved software | | | | | | | ● | ● | ● |  |
|  |  |  |  | |  | |  |  |
|  | Ensure that unauthorized software is either removed or the inventory is updated | | | | | | |  |
|  |  | in a timely manner | | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | | |  |  |  |  |
|  |  |  |  |  | | | |  |  |  |  |  |
| v7 |  | Running | |  | | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | | |  |  |  |  |



176 | P a g e

***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.*



177 | P a g e

*2.3.1 Ensure NIS Client is not installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client ( ypbind ) was used to bind a machine to an NIS server and receive the distributed configuration files.

**Rationale:**

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

**Impact:**

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

**Audit:**

Run the following command to verify that the ypbind package is not installed:



# rpm -q ypbind

package ypbind is not installed

**Remediation:**

Run the following command to remove the ypbind package:



# zypper remove ypbind



178 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | |  |  | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | |  |  |  |  |
| v7 |  | 2.6 Address unapproved software | | | | | ● | ● | ● |  |
|  |  |  | |  | |  |
|  | Ensure that unauthorized software is either removed or the inventory is updated | | | | |  |
|  |  | in a timely manner | | | | |  |  |  |  |



179 | P a g e

*2.3.2 Ensure rsh client is not installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

**Rationale:**

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

**Impact:**

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

**Audit:**

Run the following command to verify that the rsh package is not installed:



# rpm -q rsh

package rsh is not installed

**Remediation:**

Run the following command to remove the rsh package:



# zypper remove rsh



180 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | |  |  | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | |  |  |  |  |
| v7 |  | 2.6 Address unapproved software | | | | | ● | ● | ● |  |
|  |  |  | |  | |  |
|  | Ensure that unauthorized software is either removed or the inventory is updated | | | | |  |
|  |  | in a timely manner | | | | |  |  |  |  |



181 | P a g e

*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:**

Run the following command to verify that the talk package is not installed:



# rpm -q talk

package talk is not installed

**Remediation:**

Run the following command to remove the talk package:



# zypper remove talk



182 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | |  |  | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | |  |  |  |  |
| v7 |  | 2.6 Address unapproved software | | | | | ● | ● | ● |  |
|  |  |  | |  | |  |
|  | Ensure that unauthorized software is either removed or the inventory is updated | | | | |  |
|  |  | in a timely manner | | | | |  |  |  |  |



183 | P a g e

*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:**

Run the following command to verify that the telnet package is not installed:



# rpm -q telnet

package telnet is not installed

**Remediation:**

Run the following command to remove the telnet package:



# zypper remove telnet



184 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | |  |  | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | |  |  |  |  |
| v7 |  | 2.6 Address unapproved software | | | | | ● | ● | ● |  |
|  |  |  | |  | |  |
|  | Ensure that unauthorized software is either removed or the inventory is updated | | | | |  |
|  |  | in a timely manner | | | | |  |  |  |  |



185 | P a g e

*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:**

Run the following command to verify that the openldap-clients package is not installed:



# rpm -q openldap2-clients

package openldap2-clients is not installed

**Remediation:**

Run the following command to remove the openldap-clients package:



# zypper remove openldap2-clients

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | |  |  | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | |  |  |  |  |
| v7 |  | 2.6 Address unapproved software | | | | | ● | ● | ● |  |
|  |  |  | |  | |  |
|  | Ensure that unauthorized software is either removed or the inventory is updated | | | | |  |
|  |  | in a timely manner | | | | |  |  |  |  |



186 | P a g e

*2.4 Ensure nonessential services are removed or masked (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

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

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

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

**Rationale:**

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

**Audit:**

Run the following command:



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

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

**Remediation:**

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



# zypper remove <package\_name>

*OR*

*If required packages have a dependency:*

Run the following command to stop and mask the service:



# systemctl --now mask <service\_name>

**CIS Controls:**



187 | P a g e

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



188 | P a g e

***3 Network Configuration***

This section provides guidance on for securing the network configuration of the system through kernel parameters, access list control, and firewall settings.



189 | P a g e

***3.1 Disable unused network protocols and devices***

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



190 | P a g e

/etc/ssh/sshd\_config

*3.1.1 Disable IPv6 (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Although IPv6 has many advantages over IPv4, not all organizations have IPv6 or dual stack configurations implemented.

**Rationale:**

If IPv6 or dual stack is not to be used, it is recommended that IPv6 be disabled to reduce the attack surface of the system.

**Impact:**

*If IPv6 is disabled through sysctl config, SSH X11forwarding may no longer function as expected.*

We recommend that SSH X11forwarding be disabled, but if required, the following will allow for SSH X11forwarding with IPv6 disabled through sysctl config:

Add the following line the file:



AddressFamily inet

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



# systemctl restart sshd



191 | P a g e

**Audit:**

Run the following commands to verify that one of the following methods has been used to disable IPv6:

*If IPv6 is disabled through the GRUB2 config:*

Run the following command and verify no lines should be returned.

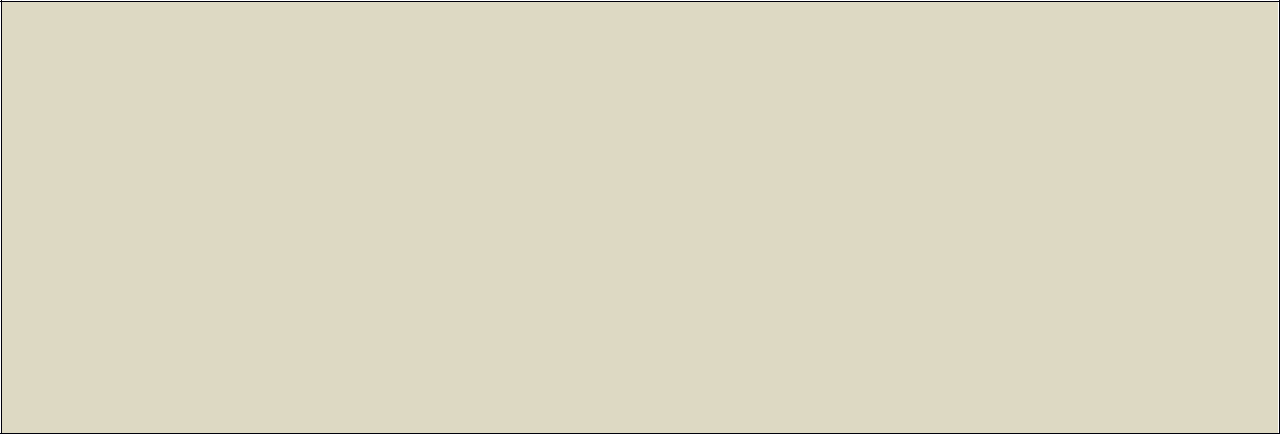


* grep "^\s\*linux" /boot/grub2/grub.cfg | grep -v ipv6.disable=1

*OR*

*If IPv6 is disabled through sysctl settings:*

Run the following commands:



* sysctl net.ipv6.conf.all.disable\_ipv6 net.ipv6.conf.all.disable\_ipv6 = 1
* sysctl net.ipv6.conf.default.disable\_ipv6 net.ipv6.conf.default.disable\_ipv6 = 1
* grep -E

'^\s\*net\.ipv6\.conf\.(all|default)\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$' /etc/sysctl.conf /etc/sysctl.d/\*.conf | cut -d: -f2

net.ipv6.conf.all.disable\_ipv6 = 1

net.ipv6.conf.default.disable\_ipv6 = 1



192 | P a g e

**Remediation:**

Use one of the two following methods to disable IPv6 on the system:

*To disable IPv6 through the GRUB2 config:*

Edit /etc/default/grub and add ipv6.disable=1 to the GRUB\_CMDLINE\_LINUX parameters:



GRUB\_CMDLINE\_LINUX="ipv6.disable=1"

Run the following command to update the grub2 configuration:



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

*OR*

*To disable IPv6 through sysctl settings:*

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



net.ipv6.conf.all.disable\_ipv6 = 1

net.ipv6.conf.default.disable\_ipv6 = 1

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv6.conf.all.disable\_ipv6=1
* sysctl -w net.ipv6.conf.default.disable\_ipv6=1
* sysctl -w net.ipv6.route.flush=1

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | |  |  | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | |  |  |  |  |
|  |  | 9.4 Apply Host-based Firewalls or Port Filtering | | | | |  |  |  |  |
|  |  |  |  | |  | |  |  |  |  |
| v7 |  | 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. | | | | |  |  |  |  |



193 | P a g e

*3.1.2 Ensure wireless interfaces are disabled (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 2 - Workstation

**Description:**

Wireless networking is used when wired networks are unavailable.

**Rationale:**

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

**Impact:**

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

**Audit:**

Run the following command to determine wireless interfaces on the system:



# iw list

Run the following command and verify wireless interfaces are active:



# ip link show up

**Remediation:**

Run the following command to disable any wireless interfaces:



# ip link set <interface> down

Disable any wireless interfaces in your network configuration.



194 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  |  |  | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | | |  |  |  |  |
| v7 |  | 15.4 Disable Wireless Access on Devices if Not Required | | | | | | |  |  | ● |  |
|  |  | |  | |  |  | |  |  |  |
|  | Disable wireless access on devices that do not have a business purpose for | | | | | | |  |  |  |
|  |  | wireless access. | | | | | | |  |  |  |  |
|  |  | 15.5 Limit Wireless Access on Client Devices | | | | | | |  |  |  |  |
|  |  |  | |  | |  | | |  |  |  |  |
| v7 |  | 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. | | | | | | |  |  |  |  |



195 | P a g e

***3.2 Network Parameters (Host Only)***

The following network parameters are intended for use if the system is to act as a host only. A system is considered host only if the system has a single interface, or has multiple interfaces but will not be configured as a router.



196 | P a g e

*3.2.1 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:**

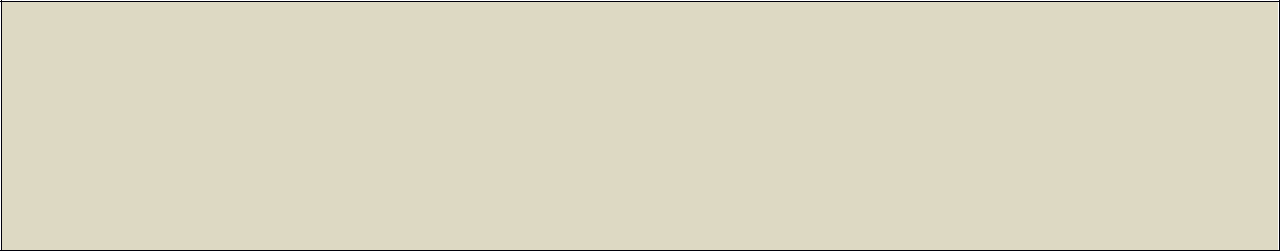
Setting the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.



197 | P a g e

**Audit:**

Run the following commands and verify output matches:

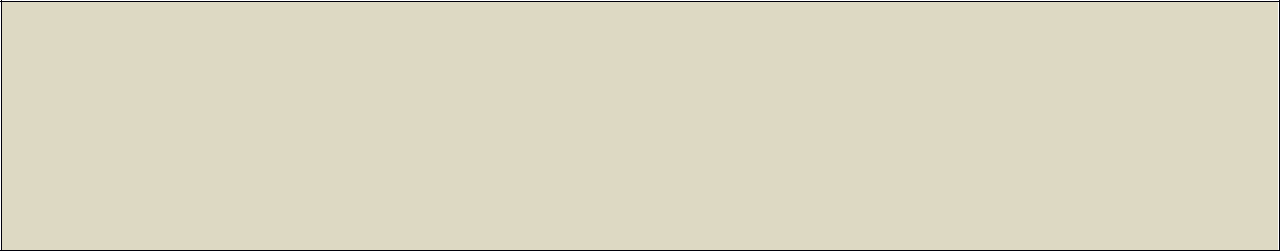


* sysctl net.ipv4.ip\_forward net.ipv4.ip\_forward = 0
* grep -E -s "^\s\*net\.ipv4\.ip\_forward\s\*=\s\*1" /etc/sysctl.conf /etc/sysctl.d/\*.conf /usr/lib/sysctl.d/\*.conf /run/sysctl.d/\*.conf

No value should be returned

*If IPv6 is enabled:*

Run the following commands and verify output matches:



* sysctl net.ipv6.conf.all.forwarding net.ipv6.conf.all.forwarding = 0
* grep -E -s "^\s\*net\.ipv6\.conf\.all\.forwarding\s\*=\s\*1" /etc/sysctl.conf /etc/sysctl.d/\*.conf /usr/lib/sysctl.d/\*.conf /run/sysctl.d/\*.conf

No value should be returned

*OR*

*Verify that IPv6 is disabled:*

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



#!/bin/bash

[ -n "$passing" ] && passing=""

[ -z "$(grep "^\s\*linux" /boot/grub2/grub.cfg | grep -v ipv6.disabled=1)" ]

&& passing="true"

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$"

/etc/sysctl.conf \

/etc/sysctl.d/\*.conf && grep -Eq

"^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" \

/etc/sysctl.conf /etc/sysctl.d/\*.conf && sysctl

net.ipv6.conf.all.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && \

sysctl net.ipv6.conf.default.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && passing="true"

if [ "$passing" = true ] ; then

echo "IPv6 is disabled on the system"

else

echo "IPv6 is enabled on the system"

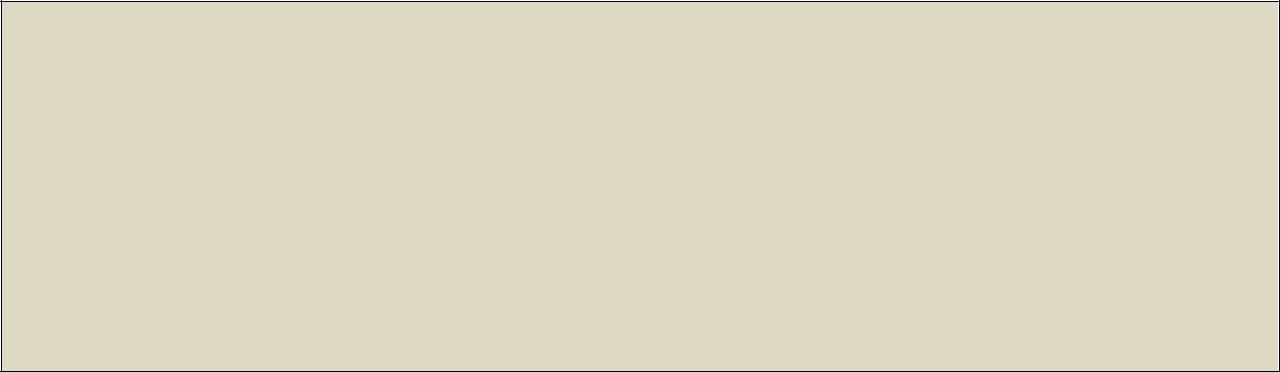
fi



198 | P a g e

**Remediation:**

Run the following commands to restore the default parameters and set the active kernel parameters:



* grep -Els "^\s\*net\.ipv4\.ip\_forward\s\*=\s\*1" /etc/sysctl.conf /etc/sysctl.d/\*.conf /usr/lib/sysctl.d/\*.conf /run/sysctl.d/\*.conf | while read filename; do sed -ri "s/^\s\*(net\.ipv4\.ip\_forward\s\*)(=)(\s\*\S+\b).\*$/# \*REMOVED\* \1/" $filename; done; sysctl -w net.ipv4.ip\_forward=0; sysctl -w net.ipv4.route.flush=1
* grep -Els "^\s\*net\.ipv6\.conf\.all\.forwarding\s\*=\s\*1" /etc/sysctl.conf /etc/sysctl.d/\*.conf /usr/lib/sysctl.d/\*.conf /run/sysctl.d/\*.conf | while read filename; do sed -ri "s/^\s\*(net\.ipv6\.conf\.all\.forwarding\s\*)(=)(\s\*\S+\b).\*$/# \*REMOVED\* \1/" $filename; done; sysctl -w net.ipv6.conf.all.forwarding=0; sysctl -w net.ipv6.route.flush=1

**CIS Controls:**

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



199 | P a g e

*3.2.2 Ensure packet redirect sending is disabled (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

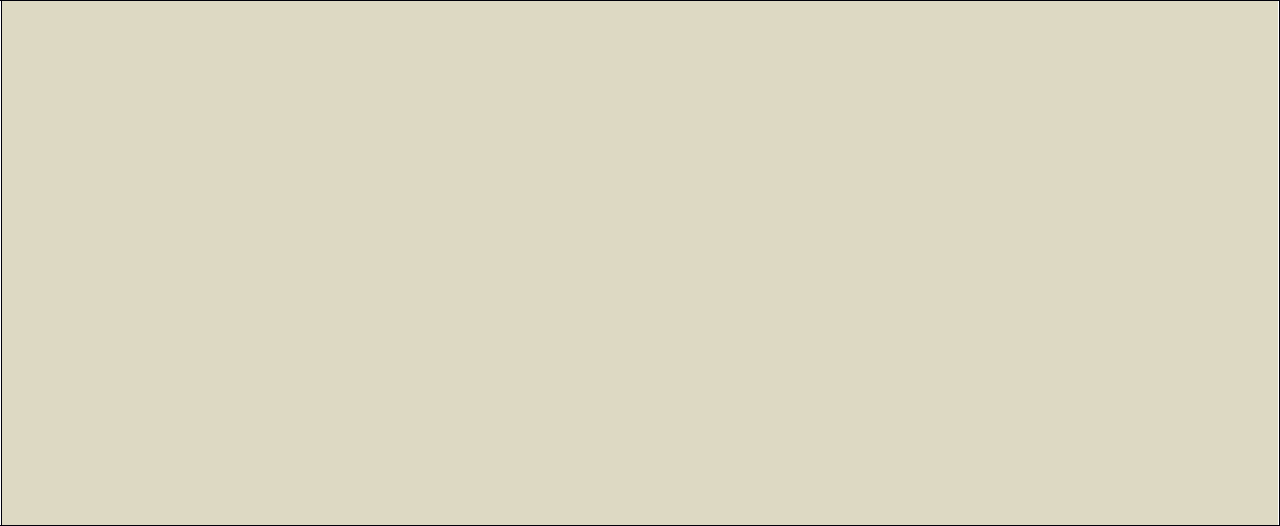
ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects.

**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.

**Audit:**

Run the following commands and verify output matches:



* sysctl net.ipv4.conf.all.send\_redirects net.ipv4.conf.all.send\_redirects = 0
* sysctl net.ipv4.conf.default.send\_redirects net.ipv4.conf.default.send\_redirects = 0
* grep "net\.ipv4\.conf\.all\.send\_redirects" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv4.conf.all.send\_redirects = 0

* grep "net\.ipv4\.conf\.default\.send\_redirects" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv4.conf.default.send\_redirects= 0



200 | P a g e

**Remediation:**

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



net.ipv4.conf.all.send\_redirects = 0 net.ipv4.conf.default.send\_redirects = 0

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv4.conf.all.send\_redirects=0
* sysctl -w net.ipv4.conf.default.send\_redirects=0
* sysctl -w net.ipv4.route.flush=1

**CIS Controls:**

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



201 | P a g e

***3.3 Network Parameters (Host and Router)***

The following network parameters are intended for use on both host only and router systems. A system acts as a router if it has at least two interfaces and is configured to perform routing functions.



202 | P a g e

*3.3.1 Ensure source routed packets are not accepted (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

**Rationale:**

Setting net.ipv4.conf.all.accept\_source\_route,

net.ipv4.conf.default.accept\_source\_route,

net.ipv6.conf.all.accept\_source\_route and

net.ipv6.conf.default.accept\_source\_route to 0 disables the system from accepting

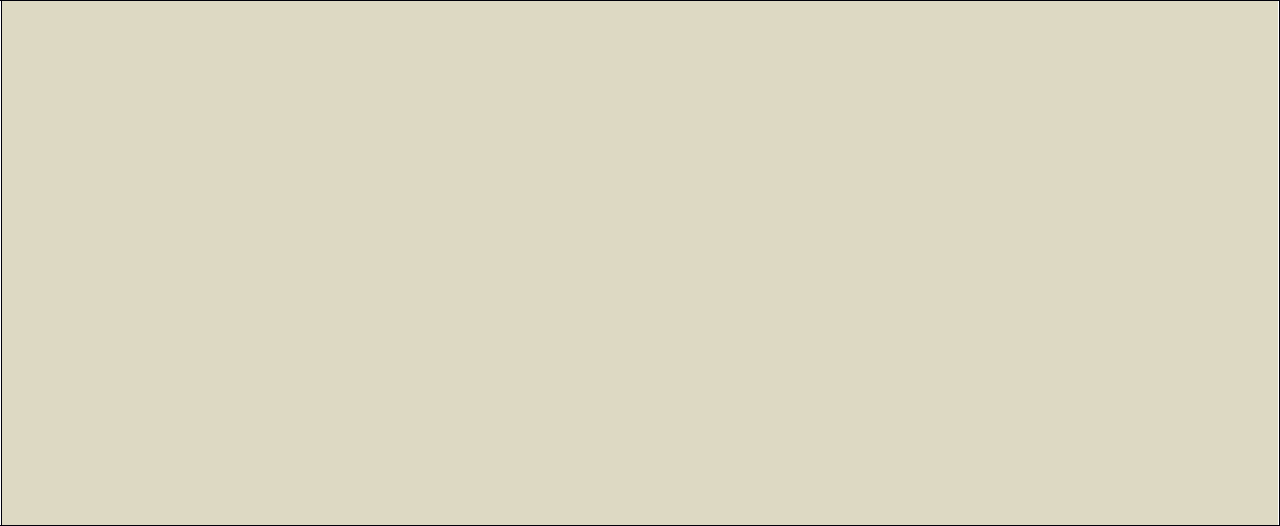
source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.



203 | P a g e

**Audit:**

Run the following commands and verify output matches:



* sysctl net.ipv4.conf.all.accept\_source\_route net.ipv4.conf.all.accept\_source\_route = 0
* sysctl net.ipv4.conf.default.accept\_source\_route net.ipv4.conf.default.accept\_source\_route = 0
* grep "net\.ipv4\.conf\.all\.accept\_source\_route" /etc/sysctl.conf /etc/sysctl.d/\*

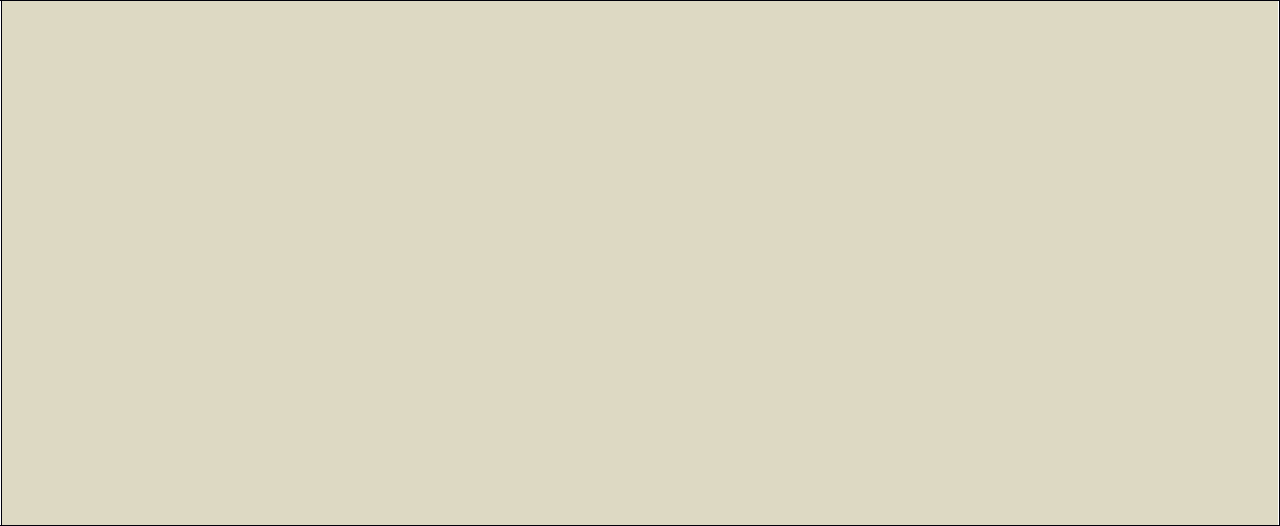
net.ipv4.conf.all.accept\_source\_route= 0

* grep "net\.ipv4\.conf\.default\.accept\_source\_route" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv4.conf.default.accept\_source\_route= 0

*If IPv6 is enabled:*

Run the following commands and verify output matches:



* sysctl net.ipv6.conf.all.accept\_source\_route net.ipv6.conf.all.accept\_source\_route = 0
* sysctl net.ipv6.conf.default.accept\_source\_route net.ipv6.conf.default.accept\_source\_route = 0
* grep "net\.ipv6\.conf\.all\.accept\_source\_route" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv4.conf.all.accept\_source\_route= 0

* grep "net\.ipv6\.conf\.default\.accept\_source\_route" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv6.conf.default.accept\_source\_route= 0



204 | P a g e

*OR*

*Verify that IPv6 is disabled:*

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



#!/bin/bash

[ -n "$passing" ] && passing=""

[ -z "$(grep "^\s\*linux" /boot/grub2/grub.cfg | grep -v ipv6.disabled=1)" ]

&& passing="true"

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$"

/etc/sysctl.conf \

/etc/sysctl.d/\*.conf && grep -Eq

"^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" \

/etc/sysctl.conf /etc/sysctl.d/\*.conf && sysctl

net.ipv6.conf.all.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && \

sysctl net.ipv6.conf.default.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && passing="true"

if [ "$passing" = true ] ; then

echo "IPv6 is disabled on the system"

else

echo "IPv6 is enabled on the system"

fi

**Remediation:**

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



net.ipv4.conf.all.accept\_source\_route = 0 net.ipv4.conf.default.accept\_source\_route = 0

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv4.conf.all.accept\_source\_route=0
* sysctl -w net.ipv4.conf.default.accept\_source\_route=0
* sysctl -w net.ipv4.route.flush=1

*If IPv6 is not disabled:*

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



net.ipv6.conf.all.accept\_source\_route = 0 net.ipv6.conf.default.accept\_source\_route = 0

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv6.conf.all.accept\_source\_route=0
* sysctl -w net.ipv6.conf.default.accept\_source\_route=0
* sysctl -w net.ipv6.route.flush=1



205 | P a g e

**CIS Controls:**

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



206 | P a g e

*3.3.2 Ensure ICMP redirects are not accepted (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting

net.ipv4.conf.all.accept\_redirects and net.ipv6.conf.all.accept\_redirects to 0,

the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

**Rationale:**

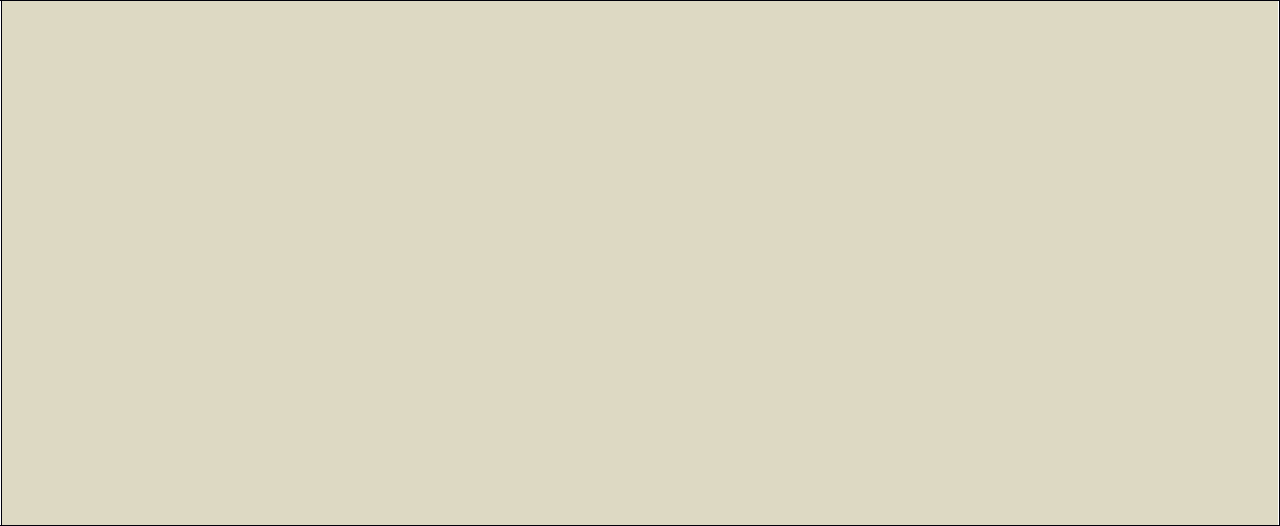
Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.



207 | P a g e

**Audit:**

Run the following commands and verify output matches:



* sysctl net.ipv4.conf.all.accept\_redirects net.ipv4.conf.all.accept\_redirects = 0
* sysctl net.ipv4.conf.default.accept\_redirects net.ipv4.conf.default.accept\_redirects = 0
* grep "net\.ipv4\.conf\.all\.accept\_redirects" /etc/sysctl.conf /etc/sysctl.d/\*

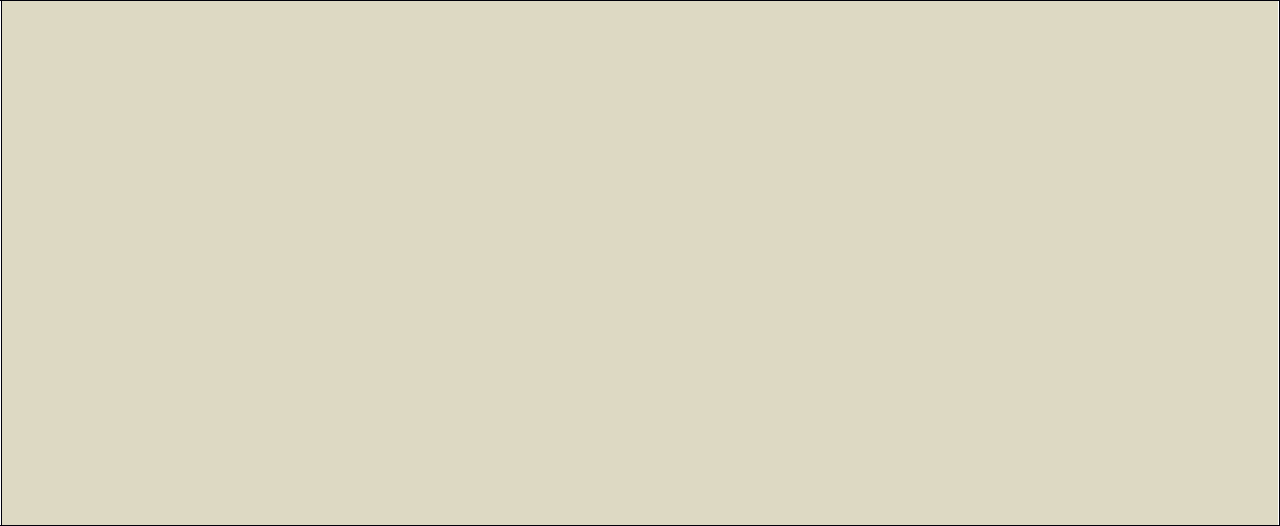
net.ipv4.conf.all.accept\_redirects= 0

* grep "net\.ipv4\.conf\.default\.accept\_redirects" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv4.conf.default.accept\_redirects= 0

*If IPv6 is not disabled:*

Run the following commands and verify output matches:



* sysctl net.ipv6.conf.all.accept\_redirects net.ipv6.conf.all.accept\_redirects = 0
* sysctl net.ipv6.conf.default.accept\_redirects net.ipv6.conf.default.accept\_redirects = 0
* grep "net\.ipv6\.conf\.all\.accept\_redirects" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv6.conf.all.accept\_redirects= 0

* grep "net\.ipv6\.conf\.default\.accept\_redirects" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv6.conf.default.accept\_redirects= 0



208 | P a g e

*OR*

*Verify IPv6 is disabled:*

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



#!/bin/bash

[ -n "$passing" ] && passing=""

[ -z "$(grep "^\s\*linux" /boot/grub2/grub.cfg | grep -v ipv6.disabled=1)" ]

&& passing="true"

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$"

/etc/sysctl.conf \

/etc/sysctl.d/\*.conf && grep -Eq

"^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" \

/etc/sysctl.conf /etc/sysctl.d/\*.conf && sysctl

net.ipv6.conf.all.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && \

sysctl net.ipv6.conf.default.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && passing="true"

if [ "$passing" = true ] ; then

echo "IPv6 is disabled on the system"

else

echo "IPv6 is enabled on the system"

fi

**Remediation:**

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



net.ipv4.conf.all.accept\_redirects = 0 net.ipv4.conf.default.accept\_redirects = 0

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv4.conf.all.accept\_redirects=0
* sysctl -w net.ipv4.conf.default.accept\_redirects=0
* sysctl -w net.ipv4.route.flush=1

*If IPv6 is not disabled:*

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



net.ipv6.conf.all.accept\_redirects = 0 net.ipv6.conf.default.accept\_redirects = 0

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv6.conf.all.accept\_redirects=0
* sysctl -w net.ipv6.conf.default.accept\_redirects=0
* sysctl -w net.ipv6.route.flush=1



209 | P a g e

**CIS Controls:**

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



210 | P a g e

*3.3.3 Ensure secure ICMP redirects are not accepted (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure.

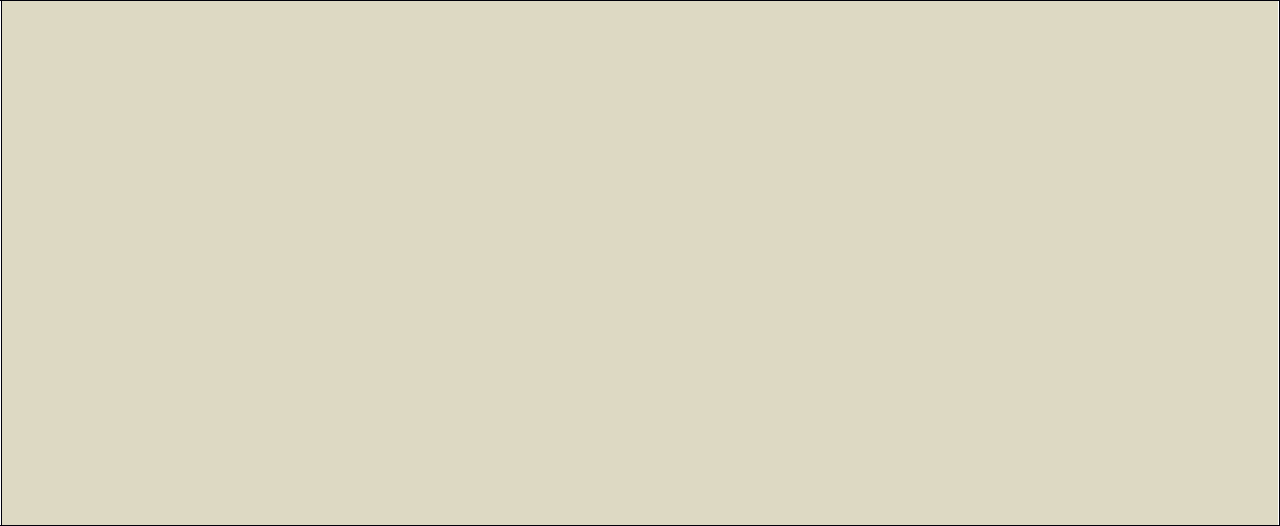
**Rationale:**

It is still possible for even known gateways to be compromised. Setting

net.ipv4.conf.all.secure\_redirects to 0 protects the system from routing table updates by possibly compromised known gateways.

**Audit:**

Run the following commands and verify output matches:



* sysctl net.ipv4.conf.all.secure\_redirects net.ipv4.conf.all.secure\_redirects = 0
* sysctl net.ipv4.conf.default.secure\_redirects net.ipv4.conf.default.secure\_redirects = 0
* grep "net\.ipv4\.conf\.all\.secure\_redirects" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv4.conf.all.secure\_redirects= 0

* grep "net\.ipv4\.conf\.default\.secure\_redirects" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv4.conf.default.secure\_redirects= 0



211 | P a g e

**Remediation:**

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



net.ipv4.conf.all.secure\_redirects = 0 net.ipv4.conf.default.secure\_redirects = 0

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv4.conf.all.secure\_redirects=0
* sysctl -w net.ipv4.conf.default.secure\_redirects=0
* sysctl -w net.ipv4.route.flush=1

**CIS Controls:**

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



212 | P a g e

*3.3.4 Ensure suspicious packets are logged (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

When enabled, this feature logs packets with un-routable source addresses to the kernel log.

**Rationale:**

Enabling this feature and logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

**Audit:**

Run the following commands and verify output matches:



* sysctl net.ipv4.conf.all.log\_martians net.ipv4.conf.all.log\_martians = 1
* sysctl net.ipv4.conf.default.log\_martians net.ipv4.conf.default.log\_martians = 1
* grep "net\.ipv4\.conf\.all\.log\_martians" /etc/sysctl.conf /etc/sysctl.d/\* net.ipv4.conf.all.log\_martians = 1
* grep "net\.ipv4\.conf\.default\.log\_martians" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv4.conf.default.log\_martians = 1

**Remediation:**

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



net.ipv4.conf.all.log\_martians = 1

net.ipv4.conf.default.log\_martians = 1

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv4.conf.all.log\_martians=1
* sysctl -w net.ipv4.conf.default.log\_martians=1
* sysctl -w net.ipv4.route.flush=1

**CIS Controls:**



213 | P a g e

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 8.5 Collect Detailed Audit Logs | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure detailed audit logging for enterprise assets containing sensitive data. | | | | |  | ● | ● |  |
| Include event source, date, username, timestamp, source addresses, destination | | | | |  |  |
|  |  |  |  |  |
|  | addresses, and other useful elements that could assist in a forensic investigation. | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Ensure that local logging has been enabled on all systems and networking devices. | | | | |  |
|  |  |  |  |  |
|  | 6.3 Enable Detailed Logging | | | | |  |  |  |  |
|  |  |  | |  | |  |  |  |  |
| v7 | Enable system logging to include detailed information such as an event source, | | | | |  | ● | ● |  |
| date, user, timestamp, source addresses, destination addresses, and other useful | | | | |  |  |
|  |  |  |  |  |
|  | elements. | | | | |  |  |  |  |



214 | P a g e

*3.3.5 Ensure broadcast ICMP requests are ignored (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

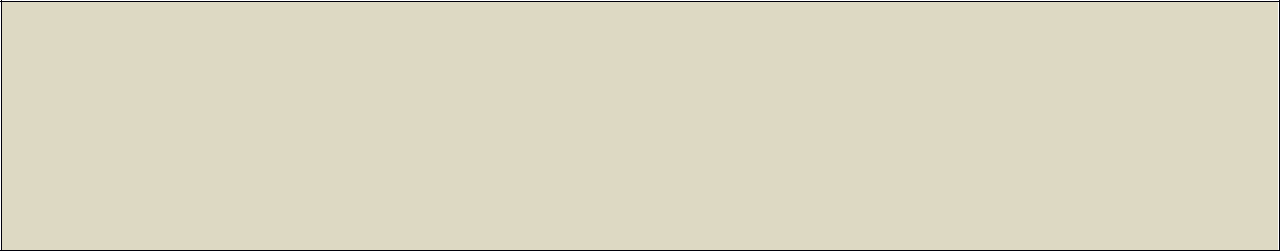
Setting net.ipv4.icmp\_echo\_ignore\_broadcasts to 1 will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses.

**Rationale:**

Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

**Audit:**

Run the following commands and verify output matches:



* sysctl net.ipv4.icmp\_echo\_ignore\_broadcasts net.ipv4.icmp\_echo\_ignore\_broadcasts = 1
* grep "net\.ipv4\.icmp\_echo\_ignore\_broadcasts" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv4.icmp\_echo\_ignore\_broadcasts = 1

**Remediation:**

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



net.ipv4.icmp\_echo\_ignore\_broadcasts = 1

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv4.icmp\_echo\_ignore\_broadcasts=1
* sysctl -w net.ipv4.route.flush=1



215 | P a g e

**CIS Controls:**

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



216 | P a g e

*3.3.6 Ensure bogus ICMP responses are ignored (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

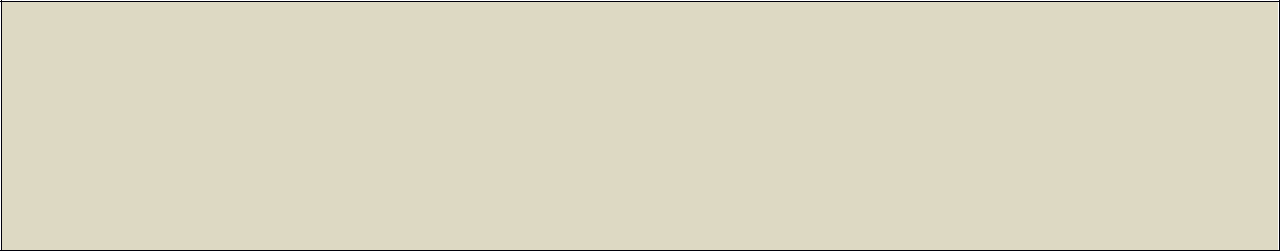
Setting icmp\_ignore\_bogus\_error\_responses to 1 prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages.

**Rationale:**

Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

**Audit:**

Run the following commands and verify output matches:



* sysctl net.ipv4.icmp\_ignore\_bogus\_error\_responses net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1
* grep "net.ipv4.icmp\_ignore\_bogus\_error\_responses" /etc/sysctl.conf /etc/sysctl.d/\*

net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1

**Remediation:**

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



net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv4.icmp\_ignore\_bogus\_error\_responses=1
* sysctl -w net.ipv4.route.flush=1



217 | P a g e

**CIS Controls:**

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



218 | P a g e

log\_martians

*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 is set).

**Rationale:**

Setting these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

**Audit:**

Run the following commands and verify output matches:



* sysctl net.ipv4.conf.all.rp\_filter net.ipv4.conf.all.rp\_filter = 1
* sysctl net.ipv4.conf.default.rp\_filter net.ipv4.conf.default.rp\_filter = 1
* grep "net\.ipv4\.conf\.all\.rp\_filter" /etc/sysctl.conf /etc/sysctl.d/\* net.ipv4.conf.all.rp\_filter = 1
* grep "net\.ipv4\.conf\.default\.rp\_filter" /etc/sysctl.conf /etc/sysctl.d/\* net.ipv4.conf.default.rp\_filter = 1



219 | P a g e

**Remediation:**

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



net.ipv4.conf.all.rp\_filter = 1

net.ipv4.conf.default.rp\_filter = 1

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv4.conf.all.rp\_filter=1
* sysctl -w net.ipv4.conf.default.rp\_filter=1
* sysctl -w net.ipv4.route.flush=1

**CIS Controls:**

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



220 | P a g e

*3.3.8 Ensure TCP SYN Cookies is enabled (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

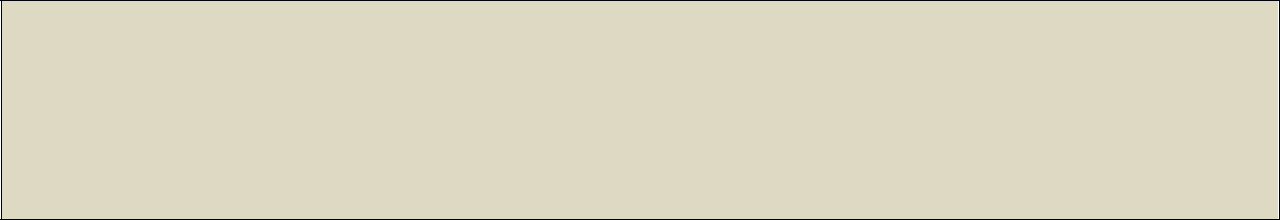
When tcp\_syncookies is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

**Rationale:**

Attackers use SYN flood attacks to perform a denial of service attacked 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



221 | P a g e

**Remediation:**

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



net.ipv4.tcp\_syncookies = 1

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv4.tcp\_syncookies=1
* sysctl -w net.ipv4.route.flush=1

**CIS Controls:**

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



222 | P a g e

*3.3.9 Ensure IPv6 router advertisements are not accepted (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

This setting disables the system's ability to accept IPv6 router advertisements.

**Rationale:**

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.



223 | P a g e

**Audit:**

Run the following commands and verify output matches:



* sysctl net.ipv6.conf.all.accept\_ra net.ipv6.conf.all.accept\_ra = 0
* sysctl net.ipv6.conf.default.accept\_ra net.ipv6.conf.default.accept\_ra = 0
* grep "net\.ipv6\.conf\.all\.accept\_ra" /etc/sysctl.conf /etc/sysctl.d/\* net.ipv6.conf.all.accept\_ra = 0
* grep "net\.ipv6\.conf\.default\.accept\_ra" /etc/sysctl.conf /etc/sysctl.d/\* net.ipv6.conf.default.accept\_ra = 0

*OR*

*Verify IPv6 is disabled:*

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



#!/bin/bash

[ -n "$passing" ] && passing=""

[ -z "$(grep "^\s\*linux" /boot/grub2/grub.cfg | grep -v ipv6.disabled=1)" ]

&& passing="true"

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$"

/etc/sysctl.conf \

/etc/sysctl.d/\*.conf && grep -Eq

"^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" \

/etc/sysctl.conf /etc/sysctl.d/\*.conf && sysctl

net.ipv6.conf.all.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && \

sysctl net.ipv6.conf.default.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && passing="true"

if [ "$passing" = true ] ; then

echo "IPv6 is disabled on the system"

else

echo "IPv6 is enabled on the system"

fi



224 | P a g e

**Remediation:**

*If IPv6 is enabled:*

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



net.ipv6.conf.all.accept\_ra = 0

net.ipv6.conf.default.accept\_ra = 0

Run the following commands to set the active kernel parameters:



* sysctl -w net.ipv6.conf.all.accept\_ra=0
* sysctl -w net.ipv6.conf.default.accept\_ra=0
* sysctl -w net.ipv6.route.flush=1

**CIS Controls:**

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



225 | P a g e

***3.4 Uncommon Network Protocols***

The Linux kernel modules support several network protocols that are not commonly used.

If these protocols are not needed, it is recommended that they be disabled in the kernel.

*Note: This should not be considered a comprehensive list of uncommon network protocols, you may wish to consider additions to those listed here for your environment.*



226 | P a g e

*3.4.1 Ensure DCCP is disabled (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

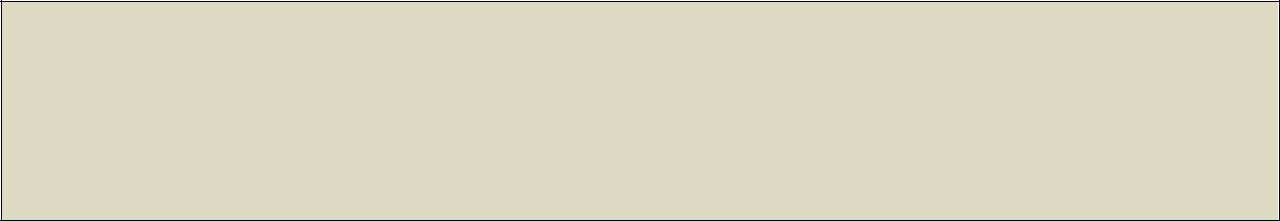
The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery.

**Rationale:**

If the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

**Audit:**

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



* modprobe -n -v dccp install /bin/true
* lsmod | grep dccp <No output>

**Remediation:**

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

*Example: vim /etc/modprobe.d/dccp.conf*

and add the following line:



install dccp /bin/true



227 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



228 | P a g e

*3.4.2 Ensure SCTP is disabled (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

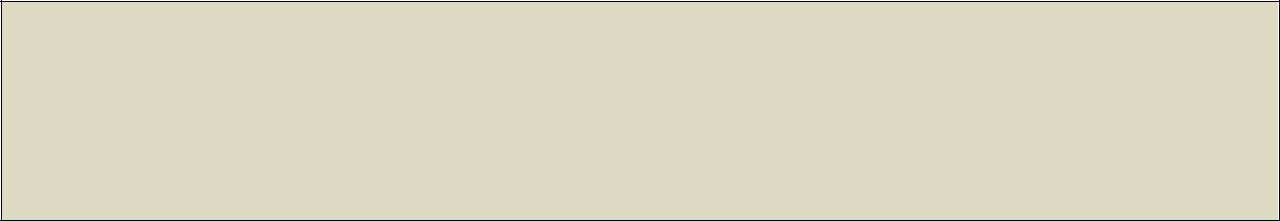
The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP.

**Rationale:**

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

**Audit:**

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



* modprobe -n -v sctp install /bin/true
* lsmod | grep sctp <No output>

**Remediation:**

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

*Example: vim /etc/modprobe.d/sctp.conf*

and add the following line:



install sctp /bin/true



229 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



230 | P a g e

***3.5 Firewall Configuration***

A firewall is a set of rules. When a data packet moves into or out of a protected network space, its contents (in particular, information about its origin, target, and the protocol it plans to use) are tested against the firewall rules to see if it should be allowed through To provide a Host Based Firewall, the Linux kernel includes support for:

* Netfilter - A set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack. Includes the ip\_tables, ip6\_tables, arp\_tables, and ebtables kernel modules. These modules are some of the significant parts of the Netfilter hook system.
* nftables - A subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames. nftables is supposed to replace certain parts of Netfilter, while keeping and reusing most of it. nftables utilizes the building blocks of the Netfilter infrastructure, such as the existing hooks into the networking stack, connection tracking system, userspace queuing component, and logging subsystem. *Is available in Linux kernels 3.13 and newer*.

In order to configure firewall rules for Netfilter or nftables, a firewall utility needs to be installed. Guidance has been included for the following firewall utilities:

* FirewallD - Provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the iptables backend. Starting in v0.6.0, FirewallD added support for acting as a front-end for the Linux kernel's netfilter framework via the nftables userspace utility, acting as an alternative to the nft command line program. firewalld supports both IPv4 and IPv6 networks and can administer separate firewall zones with varying degrees of trust as defined in zone profiles.
* nftables - Includes the nft utility for configuration of the nftables subsystem of the Linux kernel
* iptables - Includes the iptables, ip6tables, arptables and ebtables utilities for configuration Netfilter and the ip\_tables, ip6\_tables, arp\_tables, and ebtables kernel modules.

*Notes:*

* *Only one method should be used to configure a firewall on the system. Use of more than one method could produce unexpected results.*
* *This section is intended only to ensure the resulting firewall rules are in place, not how they are configured.*



231 | P a g e

***3.5.1 Configure firewalld***

*If nftables or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.*

firewalld (Dynamic Firewall Manager) provides a dynamically managed firewall with support for network/firewall “zones” to assign a level of trust to a network and its associated connections, interfaces or sources. It has support for IPv4, IPv6, Ethernet bridges and also for IPSet firewall settings. There is a separation of the runtime and permanent configuration options. It also provides an interface for services or applications to add iptables, ip6tables and ebtables rules directly. This interface can also be used by advanced users.

In the v0.6.0 release, firewalld gained support for using nftables as a firewall backend.

*Note: Configuration of a live system's firewall directly over a remote connection will often result in being locked out.*



232 | P a g e

*3.5.1.1 Ensure FirewallD is installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

firewalld is a firewall management tool for Linux operating systems. It provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the iptables backend or provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the nftables utility.

firewallD replaces iptables as the default firewall management tool. Use the firewalld utility to configure a firewall for less complex firewalls. The utility is easy to use and covers the typical use cases scenario. FirewallD supports both IPv4 and IPv6 networks and can administer separate firewall zones with varying degrees of trust as defined in zone profiles.

*Note: Starting in v0.6.0, FirewallD added support for acting as a front-end for the Linux kernel's netfilter framework via the nftables userspace utility, acting as an alternative to the nft command line program.*

**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. FirewallD is dependent on the iptables package.*

**Impact:**

Changing firewall settings while connected over the network can result in being locked out of the system.



233 | P a g e

**Audit:**

Run the following command to verify that FirewallD and iptables are installed:



# rpm -q firewalld iptables

firewalld-<version>

iptables-<version>

**Remediation:**

Run the following command to install FirewallD and iptables:



# zypper install firewalld iptables

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



234 | P a g e

*3.5.1.2 Ensure nftables is not installed or stopped and masked (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.

*Notes:*

* *Support for using nftables as the back-end for firewalld was added in release v0.6.0. In Fedora 19 Linux derivatives, firewalld utilizes iptables as it's back-end by default.*
* *firewalld may be configured as the front-end to nftables. If this case, nftables should be stopped and masked instead of removed.*

**Rationale:**

Running both firewalld and nftables may lead to conflict.

**Audit:**

Run the following commend to verify that nftables is not installed:

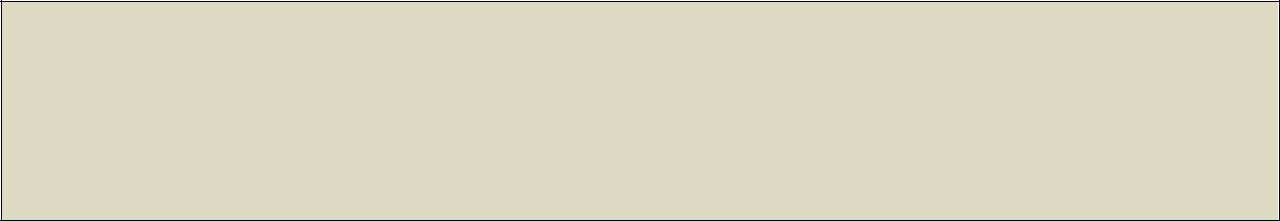


# rpm -q nftables

package nftables is not installed

*OR*

Run the following commands to verify that nftables is stopped and masked:



* systemctl status nftables | grep "Active: " | grep -v "active (running) " No output should be returned
* systemctl is-enabled nftables

masked



235 | P a g e

**Remediation:**

Run the following command to remove nftables:



# zypper remove nftables

*OR*

Run the following command to stop and mask nftables:



systemctl --now mask nftables

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.4 Implement and Manage a Firewall on Servers | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Implement and manage a firewall on servers, where supported. Example | | | | | | ● | ● | ● |  |
|  | implementations include a virtual firewall, operating system firewall, or a third- | | | | | |  |
|  |  |  |  |  |  |
|  |  | party firewall agent. | | | | | |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |
| v8 |  | Assets and Software | |  |  | | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.4 Apply Host-based Firewalls or Port Filtering | | | | | |  |  |  |  |
|  |  |  |  | |  | | |  |  |  |  |
| v7 |  | 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. | | | | | |  |  |  |  |



236 | P a g e

*3.5.1.3 Ensure firewalld service is enabled and running (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

firewalld.service enables the enforcement of firewall rules configured through

firewalld

**Rationale:**

Ensure that the firewalld.service is enabled and running to enforce firewall rules configured through firewalld

**Impact:**

Changing firewall settings while connected over network can result in being locked out of the system.

**Audit:**

Run the following command to verify that firewalld is enabled:



* systemctl is-enabled firewalld enabled

Run the following command to verify that firewalld is running



* firewall-cmd --state running

**Remediation:**

Run the following command to unmask firewalld



# systemctl unmask firewalld

Run the following command to enable and start firewalld



# systemctl --now enable firewalld



237 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



238 | P a g e

*3.5.1.4 Ensure default zone is set (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

A firewall zone defines the trust level for a connection, interface or source address binding. This is a one to many relationship, which means that a connection, interface or source can only be part of one zone, but a zone can be used for many network connections, interfaces and sources.

* The default zone is the zone that is used for everything that is not explicitly bound/assigned to another zone.
* If no zone assigned to a connection, interface or source, only the default zone is used.
* The default zone is not always listed as being used for an interface or source as it will be used for it either way. This depends on the manager of the interfaces.

Connections handled by NetworkManager are listed as NetworkManager requests to add the zone binding for the interface used by the connection. Also interfaces under control of the network service are listed also because the service requests it.

*Notes:*

* *A firewalld zone configuration file contains the information for a zone.*

1. *These are the zone description, services, ports, protocols, icmp-blocks, masquerade, forward-ports and rich language rules in an XML file format.*
   1. *The file name has to be zone\_name.xml where length of zone\_name is currently limited to 17 chars.*

* *NetworkManager binds interfaces to zones automatically*

**Rationale:**

Because the default zone is the zone that is used for everything that is not explicitly bound/assigned to another zone, it is important for the default zone to set



239 | P a g e

**Audit:**

Run the following command and verify that the default zone adheres to company policy:



# firewall-cmd --get-default-zone

**Remediation:**

Run the following command to set the default zone:



# firewall-cmd --set-default-zone=<NAME\_OF\_ZONE>

*Example:*



# firewall-cmd --set-default-zone=public

**References:**

1. <https://firewalld.org/documentation>
2. <https://firewalld.org/documentation/man-pages/firewalld.zone>

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



240 | P a g e

*3.5.1.5 Ensure network interfaces are assigned to appropriate zone (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

firewall zones define the trust level of network connections or interfaces.

*Note: The firewall in the Linux kernel is not able to handle network connections with the name shown by NetworkManager, it can only handle the network interfaces used by the connection. Because of this NetworkManager tells firewalld to assign the network interface that is used for this connection to the zone defined in the configuration of that connection. This assignment happens before the interface is used. The configuration of the connection can either be the NetworkManager configuration or also an ifcfg. For example: If the zone is not set in the configuration file, the interfaces will be assigned to the default zone defined in the firewalld configuration. If a connection has more than one interface, all of them will be supplied to firewalld. Also changes in the names of interfaces will be handled by NetworkManager and supplied to firewalld.*

**Rationale:**

A network interface not assigned to the appropriate zone can allow unexpected or undesired network traffic to be accepted on the interface.

**Impact:**

Changing firewall settings while connected over network can result in being locked out of the system.

**Audit:**

Run the following command, and verify that the interface(s) follow site policy for zone assignment



* nmcli -t connection show | awk -F: '{if($4){print $4}}' | while read INT; do firewall-cmd --get-active-zones | grep -B1 $INT; done



241 | P a g e

**Remediation:**

Run the following command to assign an interface to the approprate zone.



# firewall-cmd --zone=<Zone NAME> --change-interface=<INTERFACE NAME>

*Example:*



# firewall-cmd --zone=customezone --change-interface=eth0

**Default Value:**

If the zone is not set in the configuration file, the interfaces will be assigned to the default zone defined in the firewalld configuration

**References:**

1. <https://firewalld.org/documentation/zone/connections-interfaces-and-sources.html>

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



242 | P a g e

*3.5.1.6 Ensure unnecessary services and ports are not accepted (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Services and ports can be accepted or explicitly rejected or dropped by a zone.

For every zone, you can set a default behavior that handles incoming traffic that is not further specified. Such behavior is defined by setting the target of the zone. There are three options - default, ACCEPT, REJECT, and DROP.

* ACCEPT - you accept all incoming packets except those disabled by a specific rule.
* REJECT - you disable all incoming packets except those that you have allowed in specific rules and the source machine is informed about the rejection.
* DROP - you disable all incoming packets except those that you have allowed in specific rules and no information sent to the source machine.

**Rationale:**

To reduce the attack surface of a system, all services and ports should be blocked unless required

**Audit:**

Run the following command and review output to ensure that listed services and ports follow site policy.



* firewall-cmd --get-active-zones | awk '!/:/ {print $1}' | while read ZN; do firewall-cmd --list-all --zone=$ZN; done



243 | P a g e

**Remediation:**

Run the following command to remove an unnecessary service:



# firewall-cmd --remove-service=<service>

*Example:*



#firewall-cmd --remove-service=cockpit

Run the following command to remove an unnecessary port:



# firewall-cmd --remove-port=<port-number>/<port-type>

*Example:*



# firewall-cmd --remove-port=25/tcp

Run the following command to make new settings persistent:



# firewall-cmd --runtime-to-permanent

**References:**

1. firewalld.service(5)
2. [https://access.redhat.com/documentation/en-](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/securing_networks/using-and-configuring-firewalls_securing-networks)

[us/red\_hat\_enterprise\_linux/8/html/securing\_networks/using-and-configuring-firewalls\_securing-networks](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/securing_networks/using-and-configuring-firewalls_securing-networks)

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



244 | P a g e

***3.5.2 Configure nftables***

*If firewalld or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.*

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables. The biggest change with the successor nftables is its simplicity. With iptables, we have to configure every single rule and use the syntax which can be compared with normal commands. With nftables, the simpler syntax, much like BPF (Berkely Packet Filter) means shorter lines and less repetition. Support for nftables should also be compiled into the kernel, together with the related nftables modules. It is available in Linux kernels >= 3.13. **Please ensure that your kernel supports nftables before choosing this option.**

This section broadly assumes starting with an empty nftables firewall ruleset (established by flushing the rules with nft flush ruleset). Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot.

**Configuration of a live systems firewall directly over a remote connection will often result in being locked out**. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

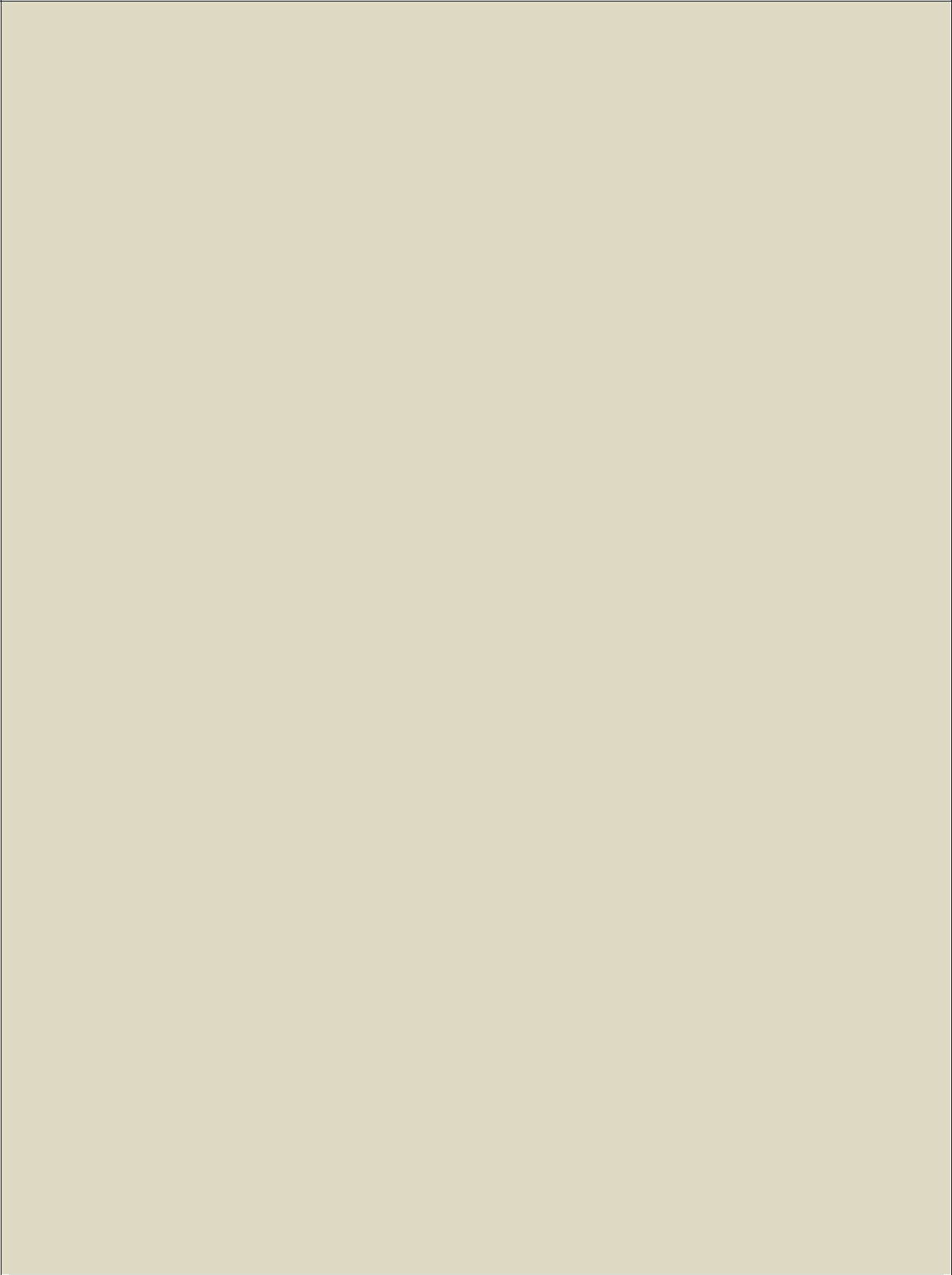
*Note: Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.*

*The following will implement the firewall rules of this section and open ICMP, IGMP, and port 22(ssh) from anywhere. Opening the ports for ICMP, IGMP, and port 22(ssh) needs to be updated in accordance with local site policy. Allow port 22(ssh) needs to be updated to only allow systems requiring ssh connectivity to connect, as per site policy.*



245 | P a g e

Save the script bellow as /etc/nftables/nftables.rules



#!/sbin/nft -f

* This nftables.rules config should be saved as /etc/nftables/nftables.rules
* flush nftables rulesset

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

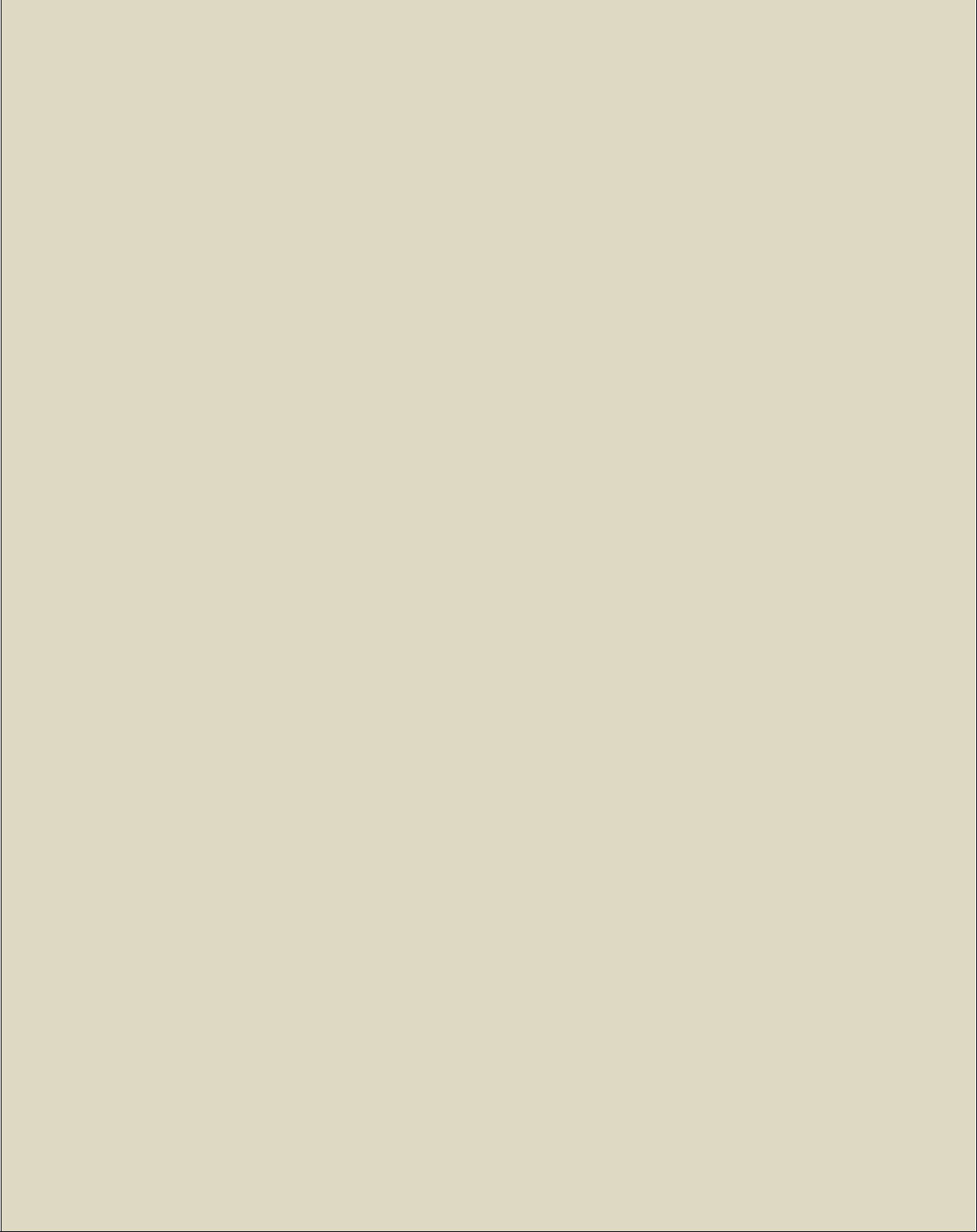
ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop ip6 saddr ::1 counter packets 0 bytes 0 drop

* 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

246 | P a g e



# 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 outbount network

packets)

chain output {

type filter hook output priority 0; policy drop;

* Ensure outbound and established connections are configured ip protocol tcp ct state established,related,new accept

ip protocol udp ct state established,related,new accept ip protocol icmp ct state established,related,new accept

}

}

Run the following command to load the file into nftables



# nft -f /etc/nftables/nftables.rules



247 | P a g e

*All changes in the nftables subsections are temporary*

To make these changes permanent:

Run the following command to create the nftables.rules file



nft list ruleset > /etc/nftables/nftables.rules

Add the following line to /etc/sysconfig/nftables.conf



include "/etc/nftables/nftables.rules"



248 | P a g e

*3.5.2.1 Ensure nftables is installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

nftables provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM) and a new nft userspace command line tool. nftables reuses the existing Netfilter subsystems such as the existing hook infrastructure, the connection tracking system, NAT, userspace queuing and logging subsystem.

*Notes:*

* *nftables is available in Linux kernel 3.13 and newer.*
* *Only one firewall utility should be installed and configured.*

**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.

**Impact:**

Changing firewall settings while connected over the network can result in being locked out of the system.

**Audit:**

Run the following command to verify that nftables is installed:



* rpm -q nftables nftables-<version>

**Remediation:**

Run the following command to install nftables



# zypper install nftables



249 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



250 | P a g e

*3.5.2.2 Ensure firewalld is not installed or stopped and masked (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

firewalld (Dynamic Firewall Manager) provides a dynamically managed firewall with support for network/firewall “zones” to assign a level of trust to a network and its associated connections, interfaces or sources. It has support for IPv4, IPv6, Ethernet bridges and also for IPSet firewall settings. There is a separation of the runtime and permanent configuration options.

**Rationale:**

Running both nftables.service and firewalld.service may lead to conflict and unexpected results.

**Audit:**

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

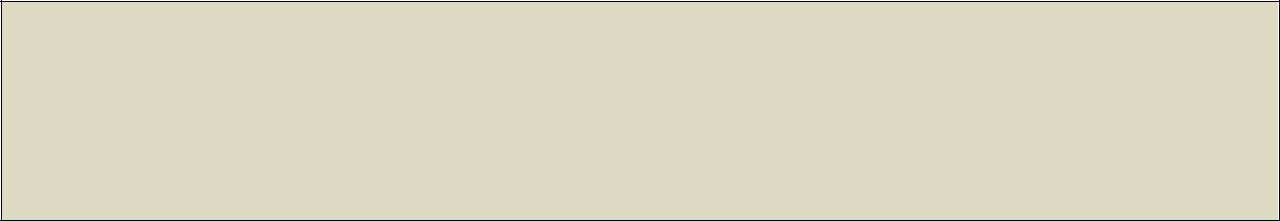


# rpm -q firewalld

package firewalld is not installed

OR

Run the following commands to verify that firewalld is stopped and masked



* systemctl status firewalld | grep "Active: " | grep -v "active (running) " No output should be returned
* systemctl is-enabled firewalld

masked



251 | P a g e

**Remediation:**

Run the following command to remove firewalld



# zypper remove firewalld

OR

Run the following command to stop and mask firewalld



# systemctl --now mask firewalld

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.4 Implement and Manage a Firewall on Servers | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Implement and manage a firewall on servers, where supported. Example | | | | | | ● | ● | ● |  |
|  | implementations include a virtual firewall, operating system firewall, or a third- | | | | | |  |
|  |  |  |  |  |  |
|  |  | party firewall agent. | | | | | |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |
| v8 |  | Assets and Software | |  |  | | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.4 Apply Host-based Firewalls or Port Filtering | | | | | |  |  |  |  |
|  |  |  |  | |  | | |  |  |  |  |
| v7 |  | 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. | | | | | |  |  |  |  |



252 | P a g e

*3.5.2.3 Ensure iptables are flushed (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 not 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



253 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



254 | P a g e

*3.5.2.4 Ensure a 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



255 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



256 | P a g e

*3.5.2.5 Ensure base chains exist (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

**Rationale:**

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

**Impact:**

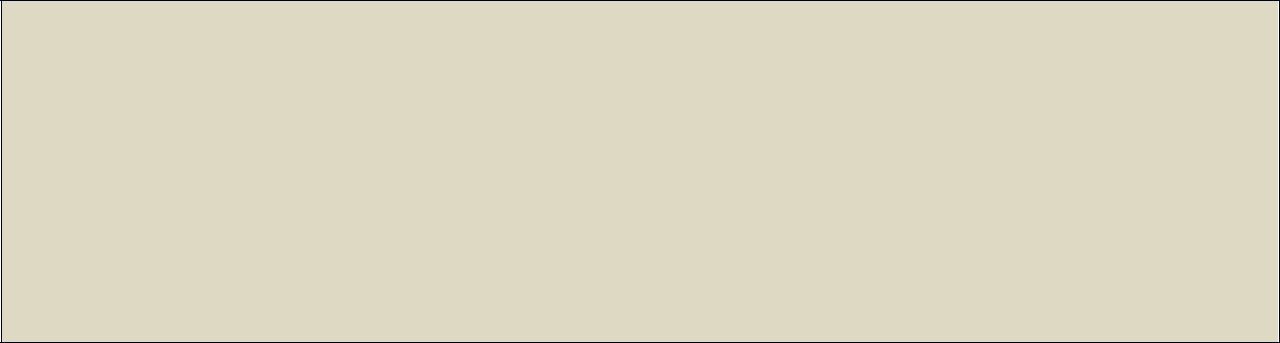
if configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

**Audit:**

Run the following commands and verify that base chains exist for INPUT, FORWARD, and

OUTPUT.



* nft list ruleset | grep 'hook input' type filter hook input priority 0;
* nft list ruleset | grep 'hook forward' type filter hook forward priority 0;
* nft list ruleset | grep 'hook output' type filter hook output priority 0;



257 | P a g e

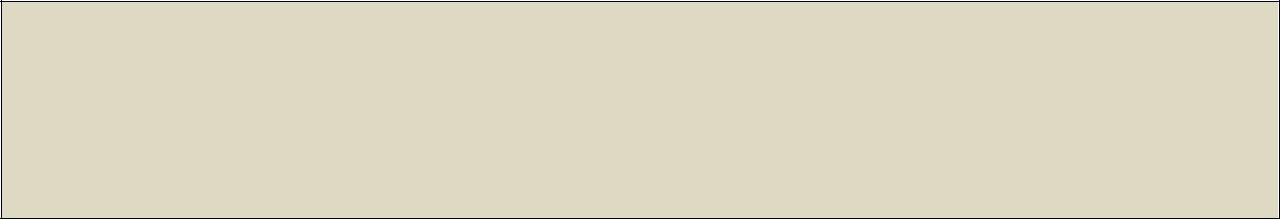
**Remediation:**

Run the following command to create the base chains:



* nft create chain inet <table name> <base chain name> { type filter hook <(input|forward|output)> priority 0 \; }

Example:



* nft create chain inet filter input { type filter hook input priority 0 \; }
* nft create chain inet filter forward { type filter hook forward priority 0 \; }
* nft create chain inet filter output { type filter hook output priority 0 \;

}

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



258 | P a g e

*3.5.2.6 Ensure 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:**

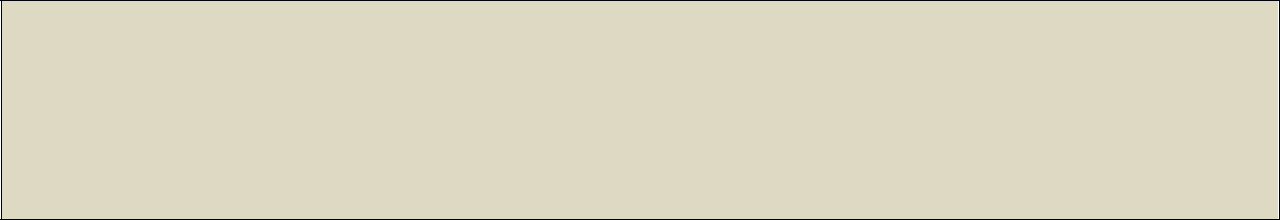
Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.



259 | P a g e

**Audit:**

Run the following commands to verify that the loopback interface is configured:



* nft list ruleset | awk '/hook input/,/}/' | grep 'iif "lo" accept' iif "lo" accept
* nft list ruleset | awk '/hook input/,/}/' | grep 'ip saddr'

ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop

*If* IPv6 is enabled:

Run the following command to verify that the IPv6 loopback interface is configured:



* nft list ruleset | awk '/hook input/,/}/' | grep 'ip6 saddr' ip6 saddr ::1 counter packets 0 bytes 0 drop

*OR*

Verify that IPv6 is disabled:

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



#!/bin/bash

[ -n "$passing" ] && passing=""

[ -z "$(grep "^\s\*linux" /boot/grub2/grub.cfg | grep -v ipv6.disabled=1)" ]

&& passing="true"

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$"

/etc/sysctl.conf \

/etc/sysctl.d/\*.conf && grep -Eq

"^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" \

/etc/sysctl.conf /etc/sysctl.d/\*.conf && sysctl

net.ipv6.conf.all.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && \

sysctl net.ipv6.conf.default.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && passing="true"

if [ "$passing" = true ] ; then

echo "IPv6 is disabled on the system"

else

echo "IPv6 is enabled on the system"

fi



260 | P a g e

**Remediation:**

Run the following commands to implement the loopback rules:



* nft add rule inet filter input iif lo accept
* nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop

*If* IPv6 is enabled:

Run the following command to implement the IPv6 loopback rules:



# nft add rule inet filter input ip6 saddr ::1 counter drop

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



261 | P a g e

*3.5.2.7 Ensure 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 folllowing 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:



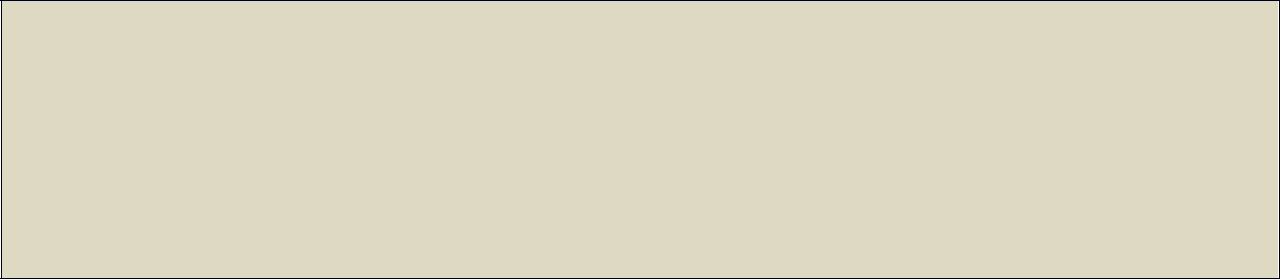
ip protocol tcp ct state established,related,new accept ip protocol udp ct state established,related,new accept ip protocol icmp ct state established,related,new accept



262 | P a g e

**Remediation:**

Configure nftables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:



* nft add rule inet filter input ip protocol tcp ct state established accept
* nft add rule inet filter input ip protocol udp ct state established accept
* nft add rule inet filter input ip protocol icmp ct state established accept
* nft add rule inet filter output ip protocol tcp ct state new,related,established accept
* nft add rule inet filter output ip protocol udp ct state new,related,established accept
* nft add rule inet filter output ip protocol icmp ct state new,related,established accept

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



263 | P a g e

*3.5.2.8 Ensure 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 traversing the network stack.

It is easier to allow acceptable usage than to block unacceptable usage.

*Note: Changing firewall settings while connected over network can result in being locked out of the system.*

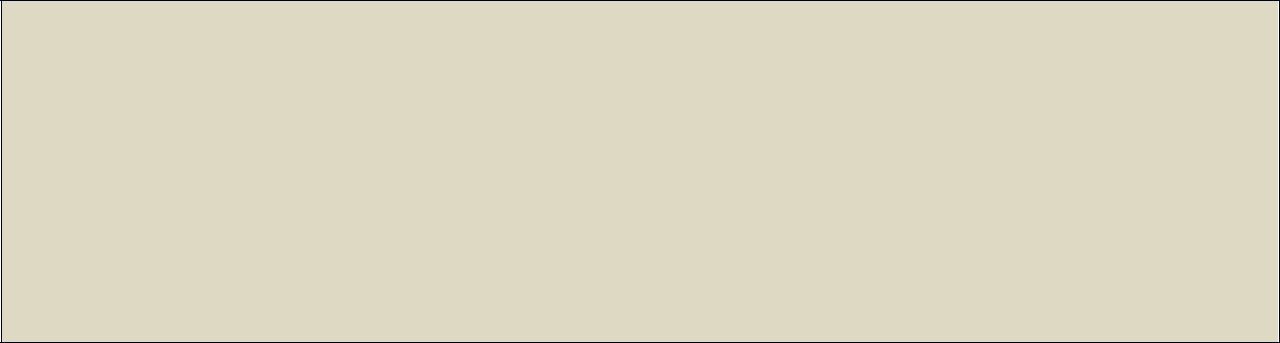
**Impact:**

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;



264 | P a g e

**Remediation:**

Run the following command for the base chains with the input, forward, and output hooks to implement a default DROP policy:



# nft chain <table family> <table name> <chain name> { policy drop \; }

Example:



* nft chain inet filter input { policy drop \; }
* nft chain inet filter forward { policy drop \; }
* nft chain inet filter output { policy drop \; }

**Default Value:**

accept

**References:**

1. Manual Page nft

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



265 | P a g e

*3.5.2.9 Ensure nftables service is enabled (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The nftables service allows for the loading of nftables rulesets during boot, or starting on the nftables service

**Rationale:**

The nftables service restores the nftables rules from the rules files referenced in the /etc/sysconfig/nftables.conf file during boot or the starting of the nftables service

**Audit:**

Run the following command and verify that the nftables service is enabled:



* systemctl is-enabled nftables enabled

**Remediation:**

Run the following command to enable the nftables service:



# systemctl enable nftables

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



266 | P a g e

*3.5.2.10 Ensure nftables rules are permanent (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames.

The nftables service reads the /etc/sysconfig/nftables.conf file for a nftables file or files to include in the nftables ruleset.

A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.

**Rationale:**

Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot



267 | P a g e

**Audit:**

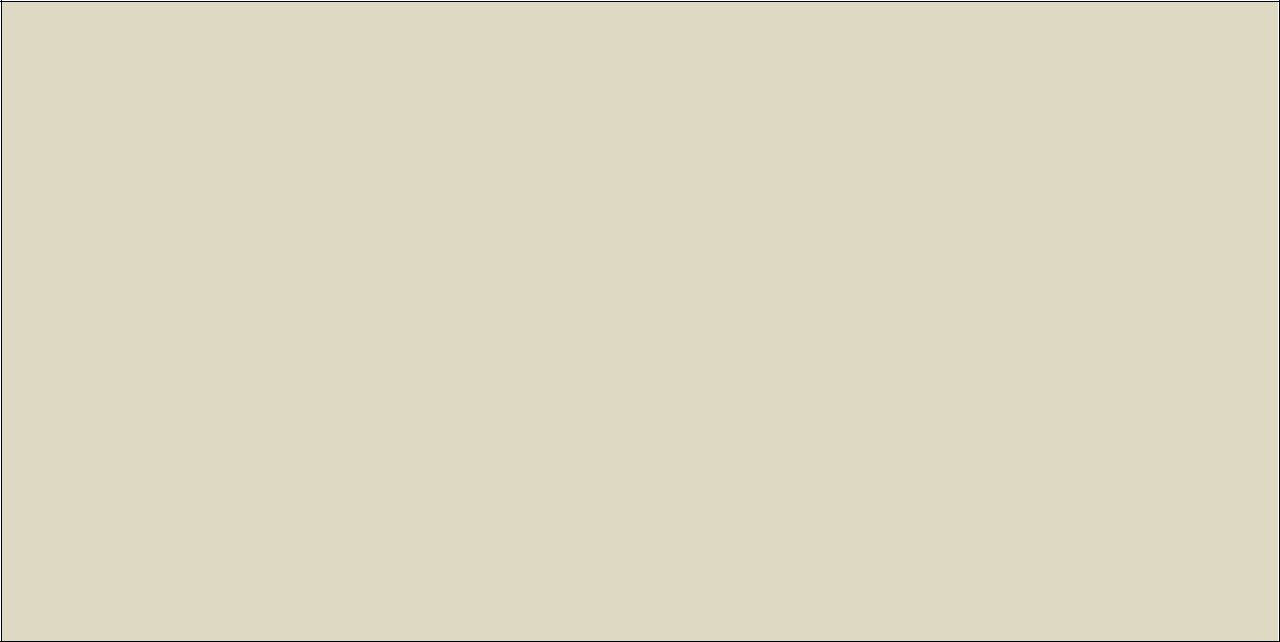
Run the following commands to verify that input, forward, and output base chains are configured to be applied to a nftables ruleset on boot:

Run the following command to verify the input base chain:



* awk '/hook input/,/}/' $(awk '$1 ~ /^\s\*include/ { gsub("\"","",$2);print $2 }' /etc/sysconfig/nftables.conf)

Output should be similar to:



type filter hook input priority 0; policy drop;

* Ensure loopback traffic is configured iif "lo" accept

ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop ip6 saddr ::1 counter packets 0 bytes 0 drop

* Ensure established connections are configured

ip protocol tcp ct state established accept ip protocol udp ct state established accept ip protocol icmp ct state established accept

* Accept port 22(SSH) traffic from anywhere tcp dport ssh accept
* Accept ICMP and IGMP from anywhere

icmpv6 type { destination-unreachable, packet-too-big, time-exceeded, parameter-problem, mld-listener-query, mld-listener-report, mld-listener-done, nd-router-solicit, nd-router-advert, nd-neighbor-solicit, nd-neighbor-advert, ind-neighbor-solicit, ind-neighbor-advert, mld2-listener-report } accept

*Note: Review the input base chain to ensure that it follows local site policy*

Run the following command to verify the forward base chain:



* awk '/hook forward/,/}/' $(awk '$1 ~ /^\s\*include/ { gsub("\"","",$2);print $2 }' /etc/sysconfig/nftables.conf)

Output should be similar to:



* Base chain for hook forward named forward (Filters forwarded network packets)

chain forward {

type filter hook forward priority 0; policy drop;

}

*Note: Review the forward base chain to ensure that it follows local site policy.*



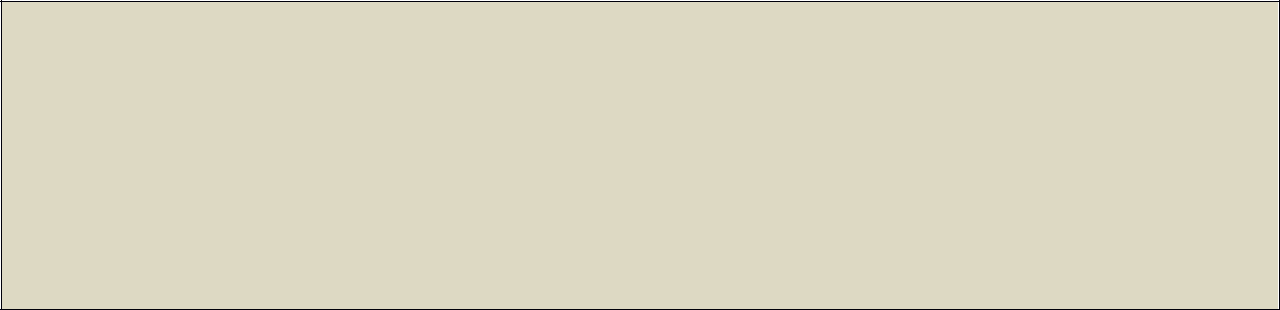
268 | P a g e

Run the following command to verify the forward base chain:



* awk '/hook output/,/}/' $(awk '$1 ~ /^\s\*include/ { gsub("\"","",$2);print $2 }' /etc/sysconfig/nftables.conf)

Output should be similar to:



# Base chain for hook output named output (Filters outbound network

packets)

chain output {

type filter hook output priority 0; policy drop;

* Ensure outbound and established connections are configured ip protocol tcp ct state established,related,new accept

ip protocol tcp ct state established,related,new accept ip protocol udp ct state established,related,new accept ip protocol icmp ct state established,related,new accept

}

*Note: Review the output base chain to ensure that it follows local site policy.*

**Remediation:**

Edit the /etc/sysconfig/nftables.conf file and un-comment or add a line with include <Absolute path to nftables rules file> for each nftables file you want included in the nftables ruleset on boot

**Example:**



# vi /etc/sysconfig/nftables.conf

Add the line:



include "/etc/nftables/nftables.rules"

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



269 | P a g e

***3.5.3 Configure iptables***

**If firewalld or nftables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.**

IPtables is an application that allows a system administrator to configure the IPv4 and IPv6 tables, chains and rules provided by the Linux kernel firewall. While several methods of configuration exist, this section is intended only to ensure the resulting IPtables rules are in place, not how they are configured. If IPv6 is in use in your environment, similar settings should be applied to the IP6tables as well.

*Note: Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.*



270 | P a g e

***3.5.3.1 Configure 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 guidance should be based over and the guidance in their respective section followed.*



271 | P a g e

*3.5.3.1.1 Ensure iptables package is installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

iptables is a utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall, implemented as different Netfilter modules, and the chains and rules it stores. Different kernel modules and programs are used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.

**Rationale:**

A method of configuring and maintaining firewall rules is necessary to configure a Host Based Firewall.

**Audit:**

Run the following command to verify that iptables is installed:



rpm -q iptables

iptables-<version>

**Remediation:**

Run the following command to install iptables



# zypper install iptables

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



272 | P a g e

*3.5.3.1.2 Ensure nftables is not installed (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 commend to verify that nftables is not installed:



# rpm -q nftables

package nftables is not installed

**Remediation:**

Run the following command to remove nftables:



# zypper remove nftables

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.4 Implement and Manage a Firewall on Servers | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Implement and manage a firewall on servers, where supported. Example | | | | | | ● | ● | ● |  |
|  | implementations include a virtual firewall, operating system firewall, or a third- | | | | | |  |
|  |  |  |  |  |  |
|  |  | party firewall agent. | | | | | |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |
| v8 |  | Assets and Software | |  |  | | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.4 Apply Host-based Firewalls or Port Filtering | | | | | |  |  |  |  |
|  |  |  |  | |  | | |  |  |  |  |
| v7 |  | 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. | | | | | |  |  |  |  |



273 | P a g e

*3.5.3.1.3 Ensure firewalld is not installed or stopped and masked (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

firewalld (Dynamic Firewall Manager) provides a dynamically managed firewall with support for network/firewall “zones” to assign a level of trust to a network and its associated connections, interfaces or sources. It has support for IPv4, IPv6, Ethernet bridges and also for IPSet firewall settings. There is a separation of the runtime and permanent configuration options.

**Rationale:**

Running iptables.service and\or ip6tables.service with firewalld.service may lead

to conflict and unexpected results.

**Audit:**

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

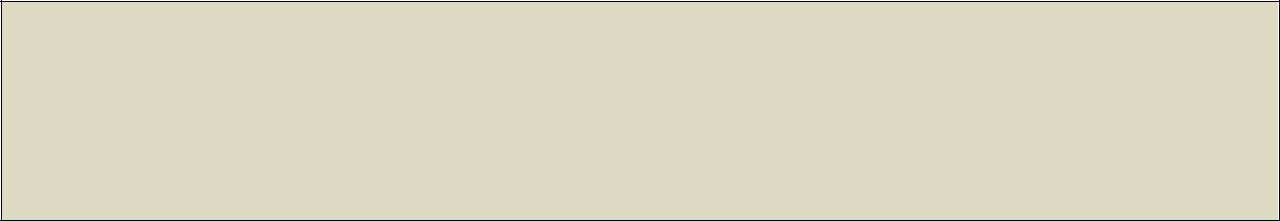


# rpm -q firewalld

package firewalld is not installed

OR

Run the following commands to verify that firewalld is stopped and masked



* systemctl status firewalld | grep "Active: " | grep -v "active (running) " No output should be returned
* systemctl is-enabled firewalld

masked



274 | P a g e

**Remediation:**

Run the following command to remove firewalld



# zypper remove firewalld

OR

Run the following command to stop and mask firewalld



# systemctl --now mask firewalld

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.4 Implement and Manage a Firewall on Servers | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Implement and manage a firewall on servers, where supported. Example | | | | | | ● | ● | ● |  |
|  | implementations include a virtual firewall, operating system firewall, or a third- | | | | | |  |
|  |  |  |  |  |  |
|  |  | party firewall agent. | | | | | |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |
| v8 |  | Assets and Software | |  |  | | |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.4 Apply Host-based Firewalls or Port Filtering | | | | | |  |  |  |  |
|  |  |  |  | |  | | |  |  |  |  |
| v7 |  | 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. | | | | | |  |  |  |  |



275 | P a g e

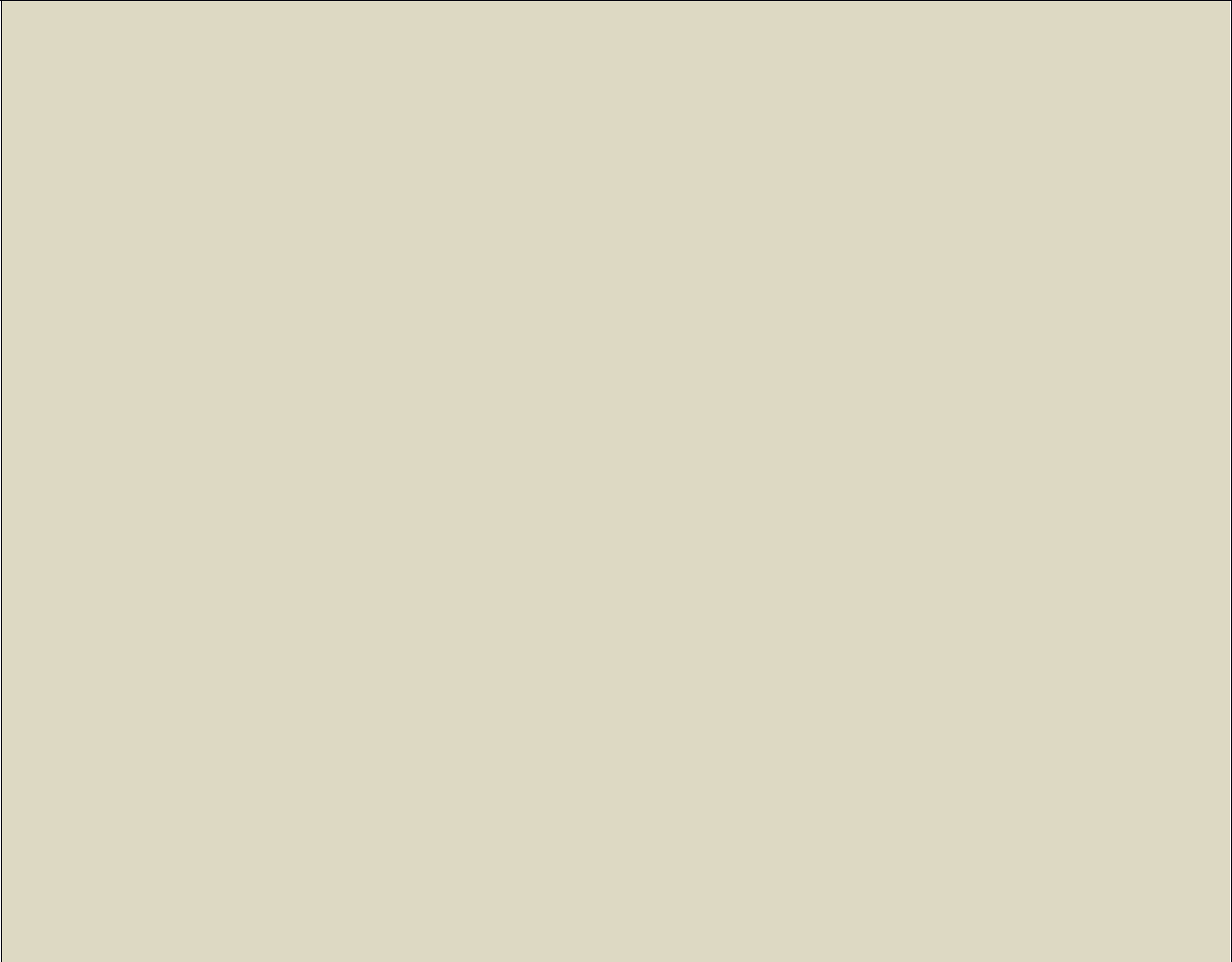
***3.5.3.2 Configure IPv4 iptables***

Iptables is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

*Notes:*

* *This section broadly assumes starting with an empty IPtables firewall ruleset (established by flushing the rules with iptables -F).*
* *Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot. The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere. This needs to be updated to only allow systems requiring ssh connectivity to connect as per site policy.*



#!/bin/bash

* Flush IPtables rules iptables -F
* Ensure default deny firewall policy iptables -P INPUT DROP

iptables -P OUTPUT DROP iptables -P FORWARD DROP

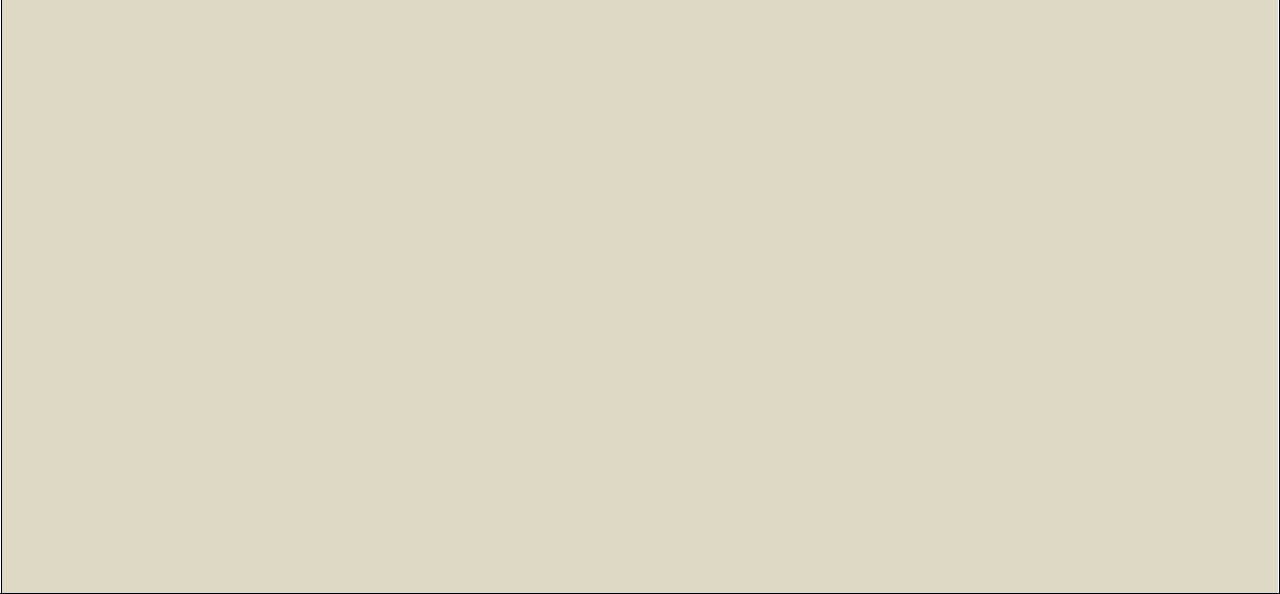
* Ensure loopback traffic is configured iptables -A INPUT -i lo -j ACCEPT iptables -A OUTPUT -o lo -j ACCEPT iptables -A INPUT -s 127.0.0.0/8 -j DROP

# Ensure outbound and established connections are configured



276 | P a g e

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



277 | P a g e

*3.5.3.2.1 Ensure default deny firewall policy (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

**Rationale:**

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

*Note: Changing firewall settings while connected over network can result in being locked out of the system.*

**Audit:**

Run the following command and verify that the policy for the INPUT, OUTPUT, and FORWARD chains is DROP or REJECT:



# iptables -L

Chain INPUT (policy DROP)

Chain FORWARD (policy DROP)

Chain OUTPUT (policy DROP)

**Remediation:**

Run the following commands to implement a default DROP policy:



* iptables -P INPUT DROP
* iptables -P OUTPUT DROP
* iptables -P FORWARD DROP

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



278 | P a g e

*3.5.3.2.2 Ensure loopback traffic is configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).

**Rationale:**

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

*Note: Changing firewall settings while connected over network can result in being locked out of the system.*

**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



279 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



280 | P a g e

*3.5.3.2.3 Ensure 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.

*Note: Changing firewall settings while connected over network can result in being locked out of the system.*

**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



281 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



282 | P a g e

*3.5.3.2.4 Ensure firewall rules exist for all open ports (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

**Rationale:**

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

*Notes:*

* *Changing firewall settings while connected over network can result in being locked out of the system.*
* *The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.*



283 | P a g e

**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



284 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.4 Implement and Manage a Firewall on Servers | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Implement and manage a firewall on servers, where supported. Example | | | | | | ● | ● | ● |  |
|  | implementations include a virtual firewall, operating system firewall, or a third- | | | | | |  |
|  |  |  |  |  |  |
|  |  | party firewall agent. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |
| v7 |  | Running | |  |  | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |
|  |  | 9.4 Apply Host-based Firewalls or Port Filtering | | | | | |  |  |  |  |
|  |  |  |  | |  | | |  |  |  |  |
| v7 |  | 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. | | | | | |  |  |  |  |



285 | P a g e

***3.5.3.3 Configure IPv6 ip6tables***

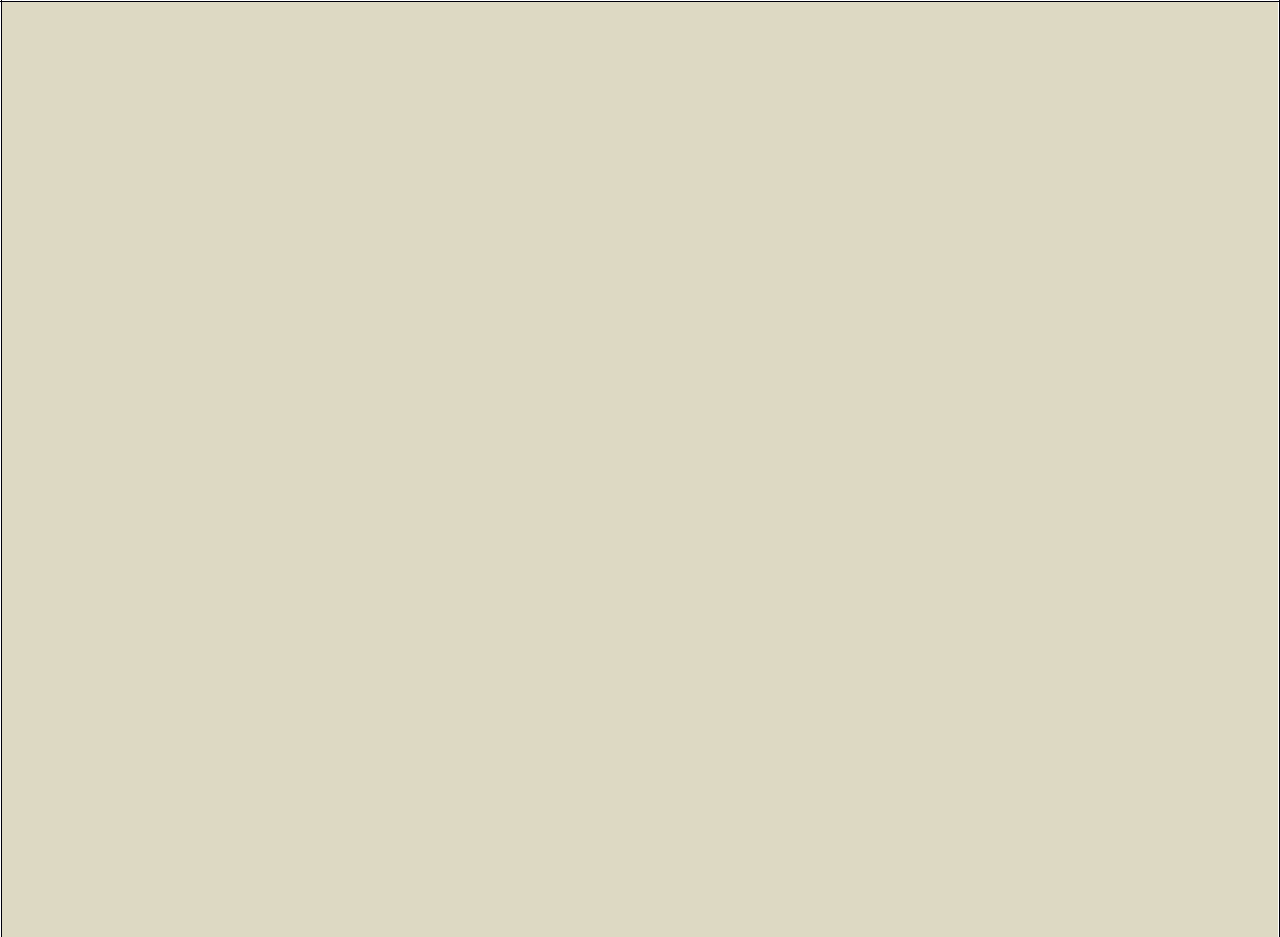
Ip6tables is used to set up, maintain, and inspect the tables of IPv6 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a ‘target’, which may be a jump to a user-defined chain in the same table.

**If IPv6 is not enabled on the system, this section can be skipped.**

*Notes:*

* *This section broadly assumes starting with an empty ip6tables firewall ruleset (established by flushing the rules with ip6tables -F).*
* *Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.*

**The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere. This needs to be updated to only allow systems requiring ssh connectivity to connect as per site policy.**



#!/bin/bash

* Flush ip6tables rules ip6tables -F
* Ensure default deny firewall policy ip6tables -P INPUT DROP

ip6tables -P OUTPUT DROP ip6tables -P FORWARD DROP

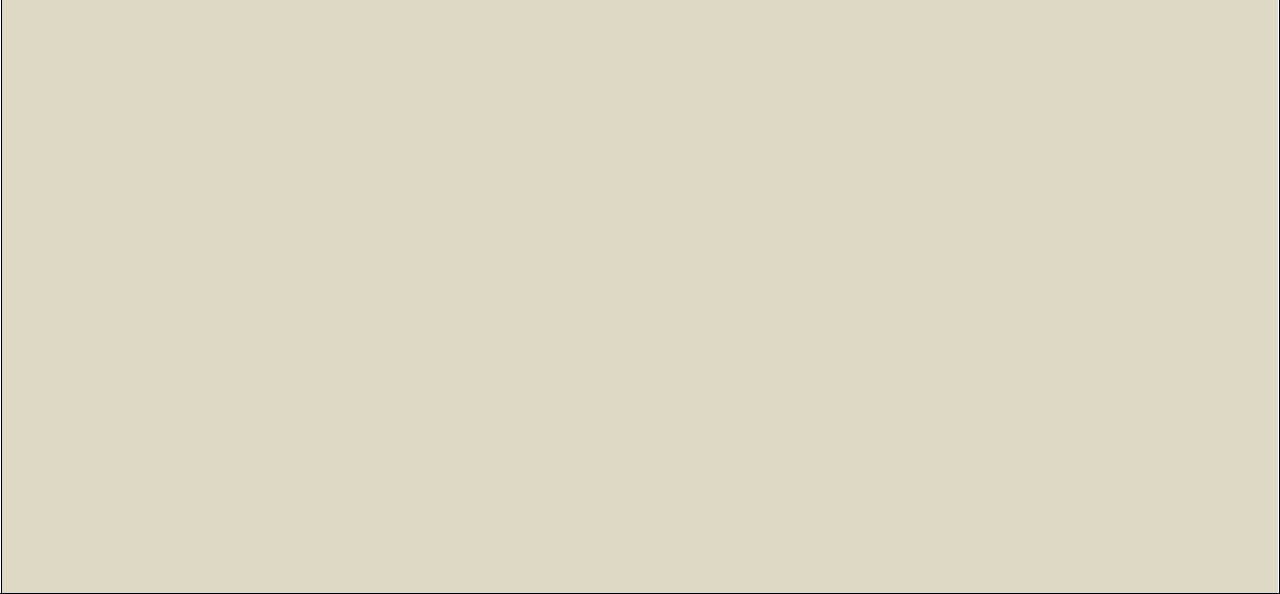
* Ensure loopback traffic is configured ip6tables -A INPUT -i lo -j ACCEPT ip6tables -A OUTPUT -o lo -j ACCEPT ip6tables -A INPUT -s ::1 -j DROP

# Ensure outbound and established connections are configured



286 | P a g e

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



287 | P a g e

*3.5.3.3.1 Ensure IPv6 default deny firewall policy (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

**Rationale:**

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

*Note: Changing firewall settings while connected over network can result in being locked out of the system.*



288 | P a g e

**Audit:**

Run the following command and verify that the policy for the INPUT, OUTPUT, and

FORWARD chains is DROP or REJECT:



# ip6tables -L

Chain INPUT (policy DROP)

Chain FORWARD (policy DROP)

Chain OUTPUT (policy DROP)

OR

Verify IPv6 is disabled:

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



#!/bin/bash

[ -n "$passing" ] && passing=""

[ -z "$(grep "^\s\*linux" /boot/grub2/grub.cfg | grep -v ipv6.disabled=1)" ]

&& passing="true"

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$"

/etc/sysctl.conf \

/etc/sysctl.d/\*.conf && grep -Eq

"^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" \

/etc/sysctl.conf /etc/sysctl.d/\*.conf && sysctl

net.ipv6.conf.all.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && \

sysctl net.ipv6.conf.default.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && passing="true"

if [ "$passing" = true ] ; then

echo "IPv6 is disabled on the system"

else

echo "IPv6 is enabled on the system"

fi

**Remediation:**

Run the following commands to implement a default DROP policy:



* ip6tables -P INPUT DROP
* ip6tables -P OUTPUT DROP
* ip6tables -P FORWARD DROP



289 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



290 | P a g e

*3.5.3.3.2 Ensure IPv6 loopback traffic is configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1).

**Rationale:**

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

*Note: Changing firewall settings while connected over network can result in being locked out of the system.*



291 | P a g e

**Audit:**

Run the following commands and verify output includes the listed rules in order (packet and byte counts may differ):

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # ip6tables | | -L INPUT -v -n | |  |  |  |  |
| Chain | INPUT | (policy DROP 0 | | packets, 0 bytes) | |  |  |
| pkts bytes target | | | prot | opt in | out | source |  |
| destination | |  |  |  |  |  |  |
| 0 | 0 | ACCEPT | all | lo | \* | ::/0 | ::/0 |
| 0 | 0 | DROP | all | \* | \* | ::1 | ::/0 |
| # ip6tables | | -L OUTPUT -v -n | |  |  |  |  |
| Chain | OUTPUT (policy DROP 0 packets, 0 bytes) | | | | |  |  |
|  | | |  |  |  |  |  |
| pkts bytes target | | | prot | opt in | out | source |  |
| destination | |  |  |  |  |  |  |
| 0 | 0 | ACCEPT | all | \* | lo | ::/0 | ::/0 |
|  |  |  |  |  |  |  |  |

OR

Verify IPv6 is disabled:

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



#!/bin/bash

[ -n "$passing" ] && passing=""

[ -z "$(grep "^\s\*linux" /boot/grub2/grub.cfg | grep -v ipv6.disabled=1)" ]

&& passing="true"

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$"

/etc/sysctl.conf \

/etc/sysctl.d/\*.conf && grep -Eq

"^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" \

/etc/sysctl.conf /etc/sysctl.d/\*.conf && sysctl

net.ipv6.conf.all.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && \

sysctl net.ipv6.conf.default.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && passing="true"

if [ "$passing" = true ] ; then

echo "IPv6 is disabled on the system"

else

echo "IPv6 is 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



292 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



293 | P a g e

*3.5.3.3.3 Ensure IPv6 outbound and established connections are configured (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Configure the firewall rules for new outbound, and established IPv6 connections.

**Rationale:**

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

*Note: Changing firewall settings while connected over network can result in being locked out of the system.*



294 | P a g e

**Audit:**

Run the following command and verify all rules for new outbound, and established connections match site policy:

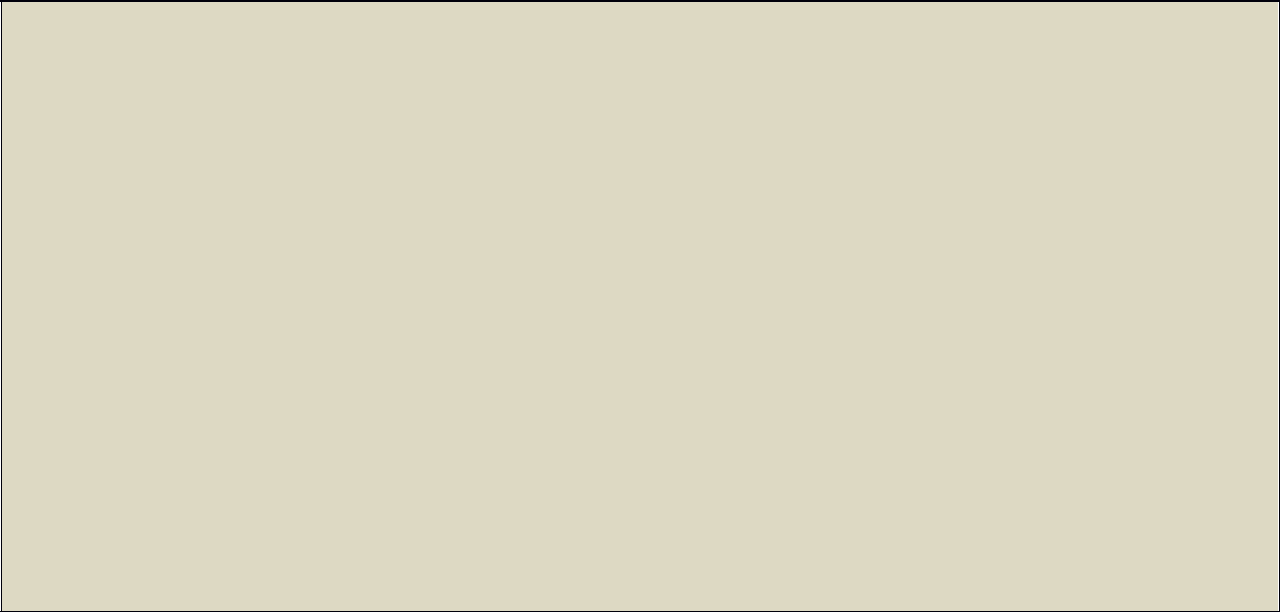


# ip6tables -L -v -n

OR

Verify IPv6 is disabled:

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



#!/bin/bash

[ -n "$passing" ] && passing=""

[ -z "$(grep "^\s\*linux" /boot/grub2/grub.cfg | grep -v ipv6.disabled=1)" ]

&& passing="true"

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$"

/etc/sysctl.conf \

/etc/sysctl.d/\*.conf && grep -Eq

"^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" \

/etc/sysctl.conf /etc/sysctl.d/\*.conf && sysctl

net.ipv6.conf.all.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && \

sysctl net.ipv6.conf.default.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && passing="true"

if [ "$passing" = true ] ; then

echo "IPv6 is disabled on the system"

else

echo "IPv6 is 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



295 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



296 | P a g e

*3.5.3.3.4 Ensure IPv6 firewall rules exist for all open ports (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

**Rationale:**

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

*Notes:*

* *Changing firewall settings while connected over network can result in being locked out of the system.*
* *The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.*



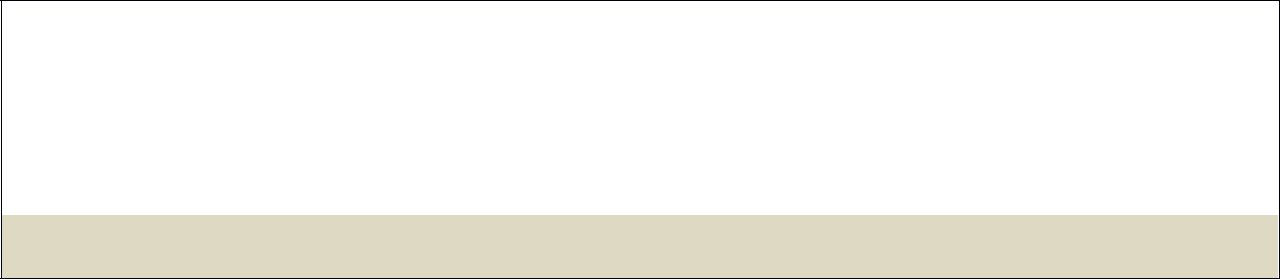
297 | P a g e

**Audit:**

Run the following command to determine open ports:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # ss -6tuln | |  |  |  |  |
| Netid | State | Recv-Q Send-Q | | Local Address:Port | Peer |
| Address:Port | |  |  |  |  |
| udp | UNCONN | 0 | 0 | ::1:123 |  |
| :::\* |  |  |  |  |  |
| udp | UNCONN | 0 | 0 | :::123 |  |
| :::\* |  |  |  |  |  |
| tcp | LISTEN | 0 | 128 | :::22 |  |
| :::\* |  |  |  |  |  |
| tcp | LISTEN | 0 | 20 | ::1:25 |  |
|  |  |  |  |  |  |
| :::\* |  |  |  |  |  |
|  |  |  |  |  |  |

Run the following command to determine firewall rules:



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # ip6tables | | -L INPUT -v -n | |  |  |  |  |
| Chain INPUT | | (policy DROP 0 packets, 0 bytes) | | | |  |  |
| pkts bytes | | target | prot opt in | | out | source |  |
| destination | |  |  |  |  |  |  |
| 0 | 0 | ACCEPT | all | lo | \* | ::/0 | ::/0 |
| 0 | 0 | DROP | all | \* | \* | ::1 | ::/0 |
| 0 | 0 | ACCEPT | tcp | \* | \* | ::/0 | ::/0 |

tcp dpt:22 state NEW

Verify all open ports listening on non-localhost addresses have at least one firewall rule. The last line identified by the "tcp dpt:22 state NEW" identifies it as a firewall rule for new connections on tcp port 22.

OR

Verify IPv6 is disabled:



298 | P a g e

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



#!/bin/bash

[ -n "$passing" ] && passing=""

[ -z "$(grep "^\s\*linux" /boot/grub2/grub.cfg | grep -v ipv6.disabled=1)" ]

&& passing="true"

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$"

/etc/sysctl.conf \

/etc/sysctl.d/\*.conf && grep -Eq

"^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" \

/etc/sysctl.conf /etc/sysctl.d/\*.conf && sysctl

net.ipv6.conf.all.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.all\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && \

sysctl net.ipv6.conf.default.disable\_ipv6 | \

grep -Eq "^\s\*net\.ipv6\.conf\.default\.disable\_ipv6\s\*=\s\*1\b(\s+#.\*)?$" && passing="true"

if [ "$passing" = true ] ; then

echo "IPv6 is disabled on the system"

else

echo "IPv6 is 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

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.4 Implement and Manage a Firewall on Servers | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Implement and manage a firewall on servers, where supported. Example | | | | ● | ● | ● |  |
| implementations include a virtual firewall, operating system firewall, or a third- | | | |  |
|  |  |  |  |  |
|  | party firewall agent. | | | |  |  |  |  |
|  | 9.4 Apply Host-based Firewalls or Port Filtering | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



299 | P a g e

***4 Logging and Auditing***

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included in most distributions.

It is recommended that rsyslog be used for logging (with logwatch providing summarization) and auditd be used for auditing (with aureport providing summarization) to automatically monitor logs for intrusion attempts and other suspicious system behavior. In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server via an encrypted connection. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices. See the ntpd(8) manual page for more information on configuring NTP.

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).*



300 | P a g e

***4.1 Configure System Accounting (auditd)***

System auditing, through auditd, allows system administrators to monitor their systems such that they can detect unauthorized access or modification of data. By default, auditd will audit system logins, account modifications, and authentication events. Events will be logged to /var/log/audit/audit.log. The recording of these events will use a modest amount of disk space on a system. If significantly more events are captured, additional on system or off system storage may need to be allocated.

*Notes:*

* *The recommendations in this section implement an audit policy that produces large quantities of logged data. In some environments it can be challenging to store or process these logs and as such they are marked as Level 2 for both Servers and Workstations.*
* *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. For 32 bit systems, only one rule is needed.*
* *Several recommendations in this section filter based off of auid>=1000 for unprivileged non-system users. Some systems may have a non-default UID\_MIN setting, consult the UID\_MIN setting in /etc/login.defs to determine the UID\_MIN setting for your system.*
* *Once all audit rules have been added to a file or files in the /etc/audit/rules.d/ directory,* ***the auditd service must be re-started, or the system rebooted, for the new rules to be included****.*
* *The audit and remediation in this section look for a 'key' value.* ***The 'key' value may be different for the audit settings on your system****.*



301 | P a g e

***4.1.1 Ensure auditing is enabled***

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.



302 | P a g e

*4.1.1.1 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 is installed:



* rpm -q audit audit-<version>

**Remediation:**

Run the following command to Install auditd



# zypper install audit

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | 8.2 Collect Audit Logs | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Collect audit logs. Ensure that logging, per the enterprise’s audit log management | | | | |  |
|  | process, has been enabled across enterprise assets. | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | ● | ● | ● |  |
|  |  | |  |  |  |
| Ensure that local logging has been enabled on all systems and networking | | | | |  |
|  | devices. | | | | |  |  |  |  |
|  | 6.3 Enable Detailed Logging | | | | |  |  |  |  |
|  |  |  | | |  |  |  |  |  |
| v7 | Enable system logging to include detailed information such as an event source, | | | | |  | ● | ● |  |
| date, user, timestamp, source addresses, destination addresses, and other useful | | | | |  |  |
|  |  |  |  |  |
|  | elements. | | | | |  |  |  |  |



303 | P a g e

*4.1.1.2 Ensure auditd service is enabled and running (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

Run the following command to verify that auditd is running:



* systemctl status auditd | grep 'Active: active (running) ' Active: active (running) since <time and date>

**Remediation:**

Run the following command to enable and start auditd:



# systemctl --now enable auditd



304 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | 8.2 Collect Audit Logs | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Collect audit logs. Ensure that logging, per the enterprise’s audit log management | | | | |  |
|  | process, has been enabled across enterprise assets. | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | ● | ● | ● |  |
|  |  | |  |  |  |
| Ensure that local logging has been enabled on all systems and networking | | | | |  |
|  | devices. | | | | |  |  |  |  |
|  | 6.3 Enable Detailed Logging | | | | |  |  |  |  |
|  |  |  | | |  |  |  |  |  |
| v7 | Enable system logging to include detailed information such as an event source, | | | | |  | ● | ● |  |
| date, user, timestamp, source addresses, destination addresses, and other useful | | | | |  |  |
|  |  |  |  |  |
|  | elements. | | | | |  |  |  |  |



305 | P a g e

*4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Configure grub 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.

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

**Audit:**

Run the following command and verify that each linux line has the audit=1 parameter set:



* grep "^\s\*linux" /boot/grub2/grub.cfg | grep -v "audit=1" Nothing should be returned

**Remediation:**

Edit /etc/default/grub and add audit=1 to GRUB\_CMDLINE\_LINUX:



GRUB\_CMDLINE\_LINUX="audit=1"

Run the following command to update the grub2 configuration:



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



306 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | 8.2 Collect Audit Logs | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Collect audit logs. Ensure that logging, per the enterprise’s audit log management | | | | |  |
|  | process, has been enabled across enterprise assets. | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | ● | ● | ● |  |
|  |  | |  |  |  |
| Ensure that local logging has been enabled on all systems and networking | | | | |  |
|  | devices. | | | | |  |  |  |  |
|  | 6.3 Enable Detailed Logging | | | | |  |  |  |  |
|  |  |  | | |  |  |  |  |  |
| v7 | Enable system logging to include detailed information such as an event source, | | | | |  | ● | ● |  |
| date, user, timestamp, source addresses, destination addresses, and other useful | | | | |  |  |
|  |  |  |  |  |
|  | elements. | | | | |  |  |  |  |



307 | P a g e

***4.1.2 Configure Data Retention***

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, auditd will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, check your site policy for audit storage requirements.



308 | P a g e

*4.1.2.1 Ensure audit log storage size is configured (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.

*Notes:*

* *The max\_log\_file parameter is measured in megabytes.*
* *Other methods of log rotation may be appropriate based on site policy. One example is time-based rotation strategies which don't have native support in auditd configurations. Manual audit of custom configurations should be evaluated for effectiveness and completeness.*

**Rationale:**

It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

**Audit:**

Run the following command and ensure output is in compliance with site policy:



* grep max\_log\_file /etc/audit/auditd.conf max\_log\_file = <MB>

**Remediation:**

Set the following parameter in /etc/audit/auditd.conf in accordance with site policy:



max\_log\_file = <MB>



309 | P a g e

**CIS Controls:**

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



310 | P a g e

*4.1.2.2 Ensure audit logs are not automatically deleted (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

The max\_log\_file\_action setting determines how to handle the audit log file reaching the max file size. A value of keep\_logs will rotate the logs but never delete old logs.

**Rationale:**

In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

**Audit:**

Run the following command and verify output matches:



* grep max\_log\_file\_action /etc/audit/auditd.conf max\_log\_file\_action = keep\_logs

**Remediation:**

Set the following parameter in /etc/audit/auditd.conf:



max\_log\_file\_action = keep\_logs

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | 8.3 Ensure Adequate Audit Log Storage | | | | |  | ● | ● |  |
|  |  |  |  |  |  |  |
| Ensure that logging destinations maintain adequate storage to comply with the | | | | |  |  |
|  | enterprise’s audit log management process. | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Ensure that local logging has been enabled on all systems and networking | | | | |  |
|  | devices. | | | | |  |  |  |  |
| v7 | 6.4 Ensure adequate storage for logs | | | | |  | ● | ● |  |
|  |  | |  | |  |  |
| Ensure that all systems that store logs have adequate storage space for the logs | | | | |  |  |
|  | generated. | | | | |  |  |  |  |



311 | P a g e

*4.1.2.3 Ensure system is disabled when audit logs are full (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

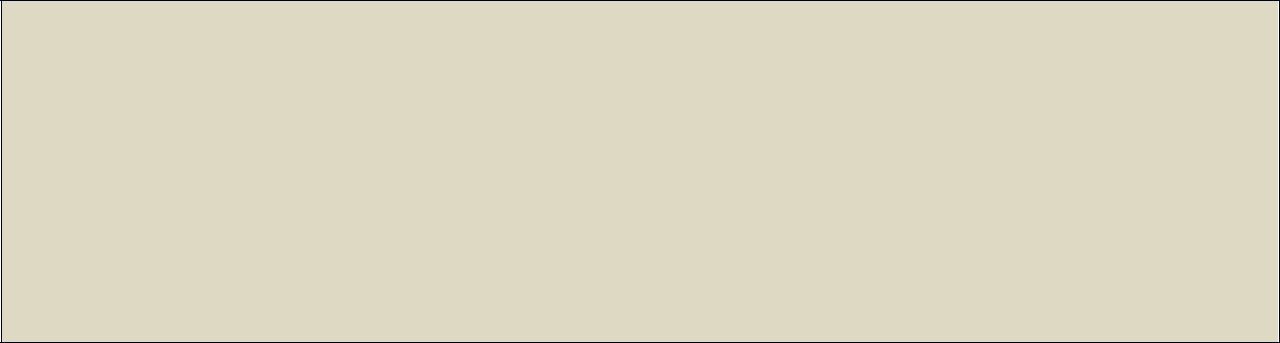
The auditd daemon can be configured to halt the system when the audit logs are full.

**Rationale:**

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

**Audit:**

Run the following commands and verify output matches:



* grep space\_left\_action /etc/audit/auditd.conf space\_left\_action = email
* grep action\_mail\_acct /etc/audit/auditd.conf action\_mail\_acct = root
* grep admin\_space\_left\_action /etc/audit/auditd.conf admin\_space\_left\_action = halt

**Remediation:**

Set the following parameters in /etc/audit/auditd.conf:



space\_left\_action = email

action\_mail\_acct = root

admin\_space\_left\_action = halt



312 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | 8.2 Collect Audit Logs | | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |  |
| Collect audit logs. Ensure that logging, per the enterprise’s audit log | | | | | |  |
|  | management process, has been enabled across enterprise assets. | | | | | |  |  |  |  |
| v8 | 8.3 Ensure Adequate Audit Log Storage | | | | | |  | ● | ● |  |
|  |  | |  |  |  |  |  |
| Ensure that logging destinations maintain adequate storage to comply with the | | | | | |  |  |
|  | enterprise’s audit log management process. | | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | | ● | ● | ● |  |
|  |  | |  |  | |  |
| Ensure that local logging has been enabled on all systems and networking | | | | | |  |
|  | devices. | | | | | |  |  |  |  |
| v7 | 6.4 Ensure adequate storage for logs | | | | | |  | ● | ● |  |
|  |  | | |  | |  |  |
| Ensure that all systems that store logs have adequate storage space for the logs | | | | | |  |  |
|  | generated. | | | | | |  |  |  |  |



313 | P a g e

*4.1.2.4 Ensure audit\_backlog\_limit is sufficient (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

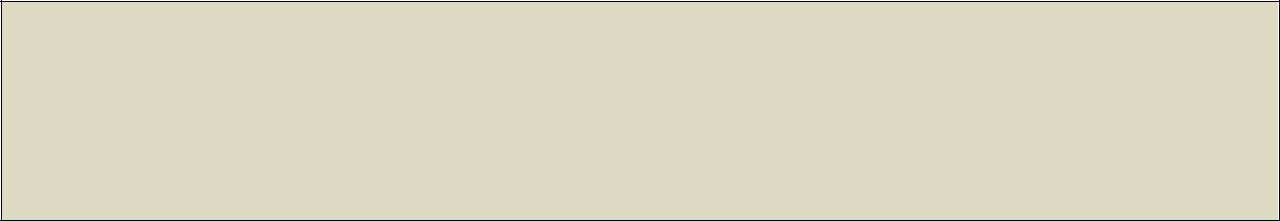
The backlog limit has a default setting of 64

**Rationale:**

During boot if audit=1, then the backlog will hold 64 records. If more that 64 records are created during boot, auditd records will be lost and potential malicious activity could go undetected.

**Audit:**

Run the following commands and verify the audit\_backlog\_limit= parameter is set to an appropriate size for your organization



* grep "^\s\*linux" /boot/grub2/grub.cfg | grep -v "audit\_backlog\_limit=" Nothing should be returned
* grep "audit\_backlog\_limit=" /boot/grub2/grub.cfg

Ensure the returned value complies with local site policy

*Recommended that this value be 8192 or larger.*

**Remediation:**

Edit /etc/default/grub and add audit\_backlog\_limit=<BACKLOG SIZE> to

GRUB\_CMDLINE\_LINUX:

*Example:*



GRUB\_CMDLINE\_LINUX="audit\_backlog\_limit=8192"

Run the following command to update the grub2 configuration:



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



314 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | 8.2 Collect Audit Logs | | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |  |
| Collect audit logs. Ensure that logging, per the enterprise’s audit log management | | | | | |  |
|  | process, has been enabled across enterprise assets. | | | | | |  |  |  |  |
| v8 | 8.3 Ensure Adequate Audit Log Storage | | | | | |  | ● | ● |  |
|  |  | |  |  |  |  |  |
| Ensure that logging destinations maintain adequate storage to comply with the | | | | | |  |  |
|  | enterprise’s audit log management process. | | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | | ● | ● | ● |  |
|  |  | |  |  | |  |
| Ensure that local logging has been enabled on all systems and networking | | | | | |  |
|  | devices. | | | | | |  |  |  |  |
|  | 6.3 Enable Detailed Logging | | | | | |  |  |  |  |
|  |  |  | | |  | |  |  |  |  |
| v7 | Enable system logging to include detailed information such as an event source, | | | | | |  | ● | ● |  |
| date, user, timestamp, source addresses, destination addresses, and other useful | | | | | |  |  |
|  |  |  |  |  |
|  | elements. | | | | | |  |  |  |  |



315 | P a g e

*4.1.3 Ensure events that modify date and time information are collected (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock\_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier "time-change"

*Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.*

**Rationale:**

Unexpected changes in system date and/or time could be a sign of malicious activity on the system.



316 | P a g e

**Audit:**

On a 32 bit system run the following commands:



* grep time-change /etc/audit/rules.d/\*.rules
* auditctl -l | grep time-change

Verify output of both matches:



-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change

-a always,exit -F arch=b32 -S clock\_settime -k time-change -w /etc/localtime -p wa -k time-change

On a 64 bit system run the following commands:

Run the following command and verify rules are in a .rules file:



# grep time-change /etc/audit/rules.d/\*.rules

Verify output matches:

|  |  |  |
| --- | --- | --- |
| /etc/audit/rules.d/time\_change.rules:-a always,exit -F | arch=b64 | -S adjtimex - |
| S settimeofday -k time-change |  |  |
| /etc/audit/rules.d/time\_change.rules:-a always,exit -F | arch=b32 | -S adjtimex - |
| S settimeofday -S stime -k time-change |  |  |
| /etc/audit/rules.d/time\_change.rules:-a always,exit -F | arch=b64 | -S |
| clock\_settime -k time-change |  |  |
| /etc/audit/rules.d/time\_change.rules:-a always,exit -F | arch=b32 | -S |
| clock\_settime -k time-change |  |  |
| /etc/audit/rules.d/time\_change.rules:-w /etc/localtime | -p wa -k | time-change |
|  |  |  |

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep time-change

Verify output matches:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| -a always,exit -F | | | arch=b64 | -S adjtimex,settimeofday -F key=time-change | |
| -a always,exit -F | | | arch=b32 | -S stime,settimeofday,adjtimex -F key=time-change | |
|  | |  |  |  |  |
| -a always,exit | | -F | arch=b64 | -S | clock\_settime -F key=time-change |
| -a | always,exit | -F | arch=b32 | -S | clock\_settime -F key=time-change |
| -w | /etc/localtime | | -p wa -k | time-change | |
|  |  |  |  |  |  |



317 | P a g e

**Remediation:**

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/time\_change.rules*

and add the following lines:



-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change

-a always,exit -F arch=b32 -S clock\_settime -k time-change -w /etc/localtime -p wa -k time-change

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/time\_change.rules*

and add the following lines:

|  |  |  |
| --- | --- | --- |
| -a always,exit -F | arch=b64 | -S adjtimex -S settimeofday -k time-change |
| -a always,exit -F | arch=b32 | -S adjtimex -S settimeofday -S stime -k time- |
| change |  |  |
| -a always,exit -F | arch=b64 | -S clock\_settime -k time-change |
| -a always,exit -F | arch=b32 | -S clock\_settime -k time-change |
| -w /etc/localtime | -p wa -k | time-change |
| **CIS Controls:** |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 8.5 Collect Detailed Audit Logs | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | 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. | | | |  |  |  |  |
|  | 5.5 Implement Automated Configuration Monitoring Systems | | | |  |  |  |  |
|  |  |  | |  |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



318 | P a g e

*4.1.4 Ensure events that modify user/group information are collected (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier "identity" in the audit log file.

*Note: Reloading the auditd config to set active settings may require a system reboot.*

**Rationale:**

Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

**Audit:**

Run the following command and verify rules are in a .rules file:



# grep identity /etc/audit/rules.d/\*.rules

Verify the output matches:



/etc/audit/rules.d/identity.rules:-w /etc/group -p wa -k identity

/etc/audit/rules.d/identity.rules:-w /etc/passwd -p wa -k identity

/etc/audit/rules.d/identity.rules:-w /etc/shadow -p wa -k identity

/etc/audit/rules.d/identity.rules:-w /etc/security/opasswd -p wa -k identity

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep identity

Verify the output matches:



-w /etc/group -p wa -k identity

-w /etc/passwd -p wa -k identity

-w /etc/shadow -p wa -k identity

-w /etc/security/opasswd -p wa -k identity

**Remediation:**



319 | P a g e

Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

*Example: vi /etc/audit/rules.d/identity.rules*

and add the following lines:



-w /etc/group -p wa -k identity

-w /etc/passwd -p wa -k identity

-w /etc/shadow -p wa -k identity

-w /etc/security/opasswd -p wa -k identity

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 8.5 Collect Detailed Audit Logs | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Configure detailed audit logging for enterprise assets containing sensitive data. | | | | |  | ● | ● |  |
|  | Include event source, date, username, timestamp, source addresses, destination | | | | |  |  |
|  |  |  |  |  |  |
|  |  | addresses, and other useful elements that could assist in a forensic investigation. | | | | |  |  |  |  |
|  |  | 4.8 Log and Alert on Changes to Administrative Group | | | | |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |
| v7 |  | Membership | |  | | |  | ● | ● |  |
|  | Configure systems to issue a log entry and alert when an account is added to or | | | | |  |  |
|  |  |  |  |  |  |
|  |  | removed from any group assigned administrative privileges. | | | | |  |  |  |  |



320 | P a g e

*4.1.5 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 monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/sysconfig/network (directory containing network interface scripts and configurations) files.

*Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.*

**Rationale:**

Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/sysconfig/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier "system-locale."



321 | P a g e

**Audit:**

If /etc/issue is not a symlink to /run/issue and the issue generator is not being used to create a volatile banner file:

On a 32 bit system run the following commands:



* grep system-locale /etc/audit/rules.d/\*.rules
* auditctl -l | grep system-locale

Verify output of both matches:



-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale -w /etc/issue -p wa -k system-locale

-w /etc/issue.net -p wa -k system-locale -w /etc/hosts -p wa -k system-locale

-w /etc/sysconfig/network -p wa -k system-locale

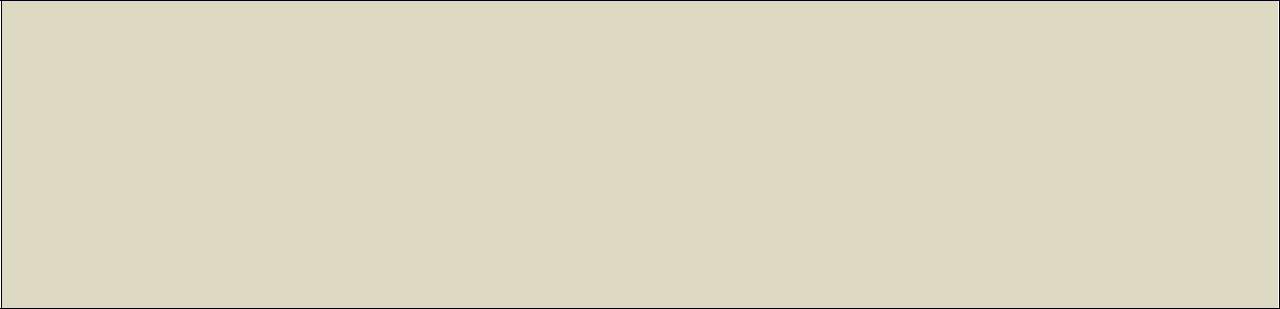
On a 64 bit system run the following commands:

Run the following command and verify rules are in a .rules file:



# grep system-locale /etc/audit/rules.d/\*.rules

Verify output matches:



/etc/audit/rules.d/system-locale.rules:-a always,exit -F arch=b64 -S

sethostname -S setdomainname -k system-locale

/etc/audit/rules.d/system-locale.rules:-a always,exit -F arch=b32 -S

sethostname -S setdomainname -k system-locale

/etc/audit/rules.d/system-locale.rules:-w /etc/issue -p wa -k system-locale

/etc/audit/rules.d/system-locale.rules:-w /etc/issue.net -p wa -k system-

locale

/etc/audit/rules.d/system-locale.rules:-w /etc/hosts -p wa -k system-locale

/etc/audit/rules.d/system-locale.rules:-w /etc/sysconfig/network -p wa -k system-locale

Run the following command and verify the rules are in the running 'auditd' config:



# auditctl -l | grep system-locale

Verify output matches:



-a always,exit -F arch=b64 -S sethostname,setdomainname -F key=system-locale -a always,exit -F arch=b32 -S sethostname,setdomainname -F key=system-locale -w /etc/issue -p wa -k system-locale

-w /etc/issue.net -p wa -k system-locale -w /etc/hosts -p wa -k system-locale

-w /etc/sysconfig/network -p wa -k system-locale



322 | P a g e

If the issue generator service is enabled then /etc/issue is a symlink and /run/issue should be verified instead:

On a 32 bit system run the following commands:



* grep system-locale /etc/audit/rules.d/\*.rules
* auditctl -l | grep system-locale

Verify output of both matches:



-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale -w /run/issue -p wa -k system-locale

-w /etc/issue.net -p wa -k system-locale -w /etc/hosts -p wa -k system-locale

-w /etc/sysconfig/network -p wa -k system-locale

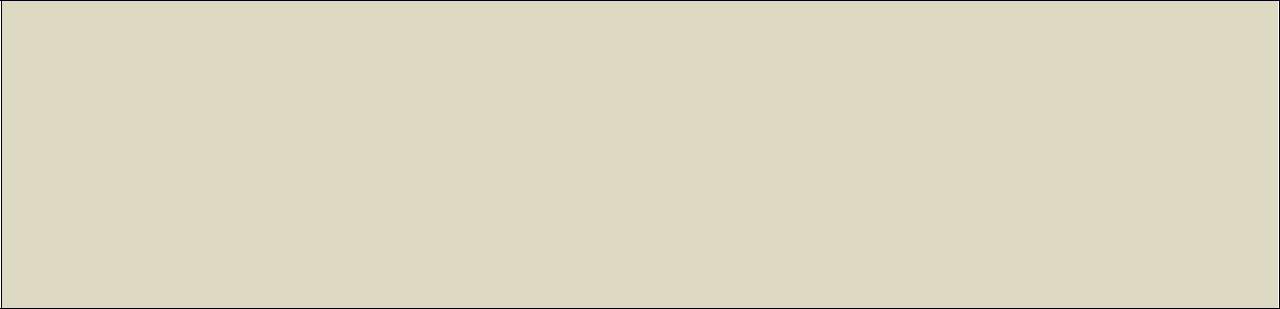
On a 64 bit system run the following commands:

Run the following command and verify rules are in a .rules file:



# grep system-locale /etc/audit/rules.d/\*.rules

Verify output matches:



/etc/audit/rules.d/system-locale.rules:-a always,exit -F arch=b64 -S

sethostname -S setdomainname -k system-locale

/etc/audit/rules.d/system-locale.rules:-a always,exit -F arch=b32 -S

sethostname -S setdomainname -k system-locale

/etc/audit/rules.d/system-locale.rules:-w /run/issue -p wa -k system-locale

/etc/audit/rules.d/system-locale.rules:-w /etc/issue.net -p wa -k system-

locale

/etc/audit/rules.d/system-locale.rules:-w /etc/hosts -p wa -k system-locale

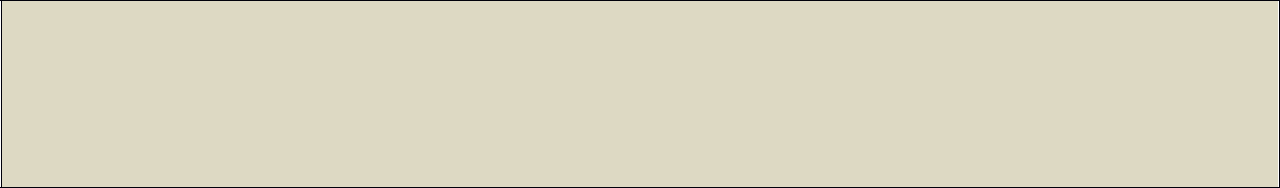
/etc/audit/rules.d/system-locale.rules:-w /etc/sysconfig/network -p wa -k system-locale

Run the following command and verify the rules are in the running 'auditd' config:



# auditctl -l | grep system-locale

Verify output matches:



-a always,exit -F arch=b64 -S sethostname,setdomainname -F key=system-locale -a always,exit -F arch=b32 -S sethostname,setdomainname -F key=system-locale -w /run/issue -p wa -k system-locale

-w /etc/issue.net -p wa -k system-locale -w /etc/hosts -p wa -k system-locale

-w /etc/sysconfig/network -p wa -k system-locale



323 | P a g e

**Remediation:**

\_If /etc/issue is not a symlink to /run/issue and the issue generator is not being used to create a volatile banner file:

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/system\_locale.rules*

and add the following lines:



-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale -w /etc/issue -p wa -k system-locale

-w /etc/issue.net -p wa -k system-locale -w /etc/hosts -p wa -k system-locale

-w /etc/sysconfig/network -p wa -k system-locale

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/system\_locale.rules*

and add the following lines:



-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale -a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale -w /etc/issue -p wa -k system-locale

-w /etc/issue.net -p wa -k system-locale -w /etc/hosts -p wa -k system-locale

-w /etc/sysconfig/network -p wa -k system-locale

If the issue generator service is enabled then /etc/issue is a symlink and /run/issue should be monitored instead:

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/system\_locale.rules*

and add the following lines:



-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale -w /run/issue -p wa -k system-locale

-w /etc/issue.net -p wa -k system-locale -w /etc/hosts -p wa -k system-locale

-w /etc/sysconfig/network -p wa -k system-locale



324 | P a g e

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/system\_locale.rules*

and add the following lines:



-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale -a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale -w /run/issue -p wa -k system-locale

-w /etc/issue.net -p wa -k system-locale -w /etc/hosts -p wa -k system-locale

-w /etc/sysconfig/network -p wa -k system-locale

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 8.5 Collect Detailed Audit Logs | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | 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. | | | | |  |  |  |  |
|  | 5.5 Implement Automated Configuration Monitoring Systems | | | | |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |
| v7 | Utilize a Security Content Automation Protocol (SCAP) compliant configuration | | | | |  | ● | ● |  |
| monitoring system to verify all security configuration elements, catalog approved | | | | |  |  |
|  |  |  |  |  |
|  | exceptions, and alert when unauthorized changes occur. | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Ensure that local logging has been enabled on all systems and networking devices. | | | | |  |
|  |  |  |  |  |



325 | P a g e

*4.1.6 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Monitor SELinux mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux/ and /usr/share/selinux/ directories.

*Notes:*

* *If a different Mandatory Access Control method is used, changes to the corresponding directories should be audited.*
* *Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.*

**Rationale:**

Changes to files in the /etc/selinux/ and /usr/share/selinux/ directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.



326 | P a g e

**Audit:**

Run the following commands:

Run the following command and verify rules are in a .rules file:



# grep MAC-policy /etc/audit/rules.d/\*.rules

Verify output matches:



/etc/audit/rules.d/MAC\_policy.rules:-w /etc/selinux/ -p wa -k MAC-policy /etc/audit/rules.d/MAC\_policy.rules:-w /usr/share/selinux/ -p wa -k MAC-policy

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep MAC-policy

Verify output matches:



-w /etc/selinux/ -p wa -k MAC-policy

-w /usr/share/selinux/ -p wa -k MAC-policy

**Remediation:**

Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

*Example: vi /etc/audit/rules.d/MAC\_policy.rules*

and add the following lines:



-w /etc/selinux/ -p wa -k MAC-policy

-w /usr/share/selinux/ -p wa -k MAC-policy

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 8.5 Collect Detailed Audit Logs | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | 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. | | | |  |  |  |  |
|  | 5.5 Implement Automated Configuration Monitoring Systems | | | |  |  |  |  |
|  |  |  | |  |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



327 | P a g e

*4.1.7 Ensure login and logout events are collected (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Monitor login and logout events. The parameters below track changes to files associated with login/logout events.

* The file /var/log/faillog tracks failed events from login.
* The file /var/log/lastlog maintain records of the last time a user successfully logged in.
* The file /var/log/tallylog maintains records of failures via the pam\_tally2 module

*Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.*

**Rationale:**

Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.



328 | P a g e

**Audit:**

Run the following commands:

Run the following command and verify rules are in a .rules file:



# grep logins /etc/audit/rules.d/\*.rules

Verify output matches:



/etc/audit/rules.d/logins.rules:-w /var/log/faillog -p wa -k logins

/etc/audit/rules.d/logins.rules:-w /var/log/lastlog -p wa -k logins

/etc/audit/rules.d/logins.rules:-w /var/log/tallylog -p wa -k logins

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep logins

Verify output matches:



-w /var/log/faillog -p wa -k logins

-w /var/log/lastlog -p wa -k logins

-w /var/log/tallylog -p wa -k logins

**Remediation:**

Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

*Example: vi /etc/audit/rules.d/logins.rules*

and add the following lines:



-w /var/log/faillog -p wa -k logins

-w /var/log/lastlog -p wa -k logins

-w /var/log/tallylog -p wa -k logins



329 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 8.5 Collect Detailed Audit Logs | | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Configure detailed audit logging for enterprise assets containing sensitive data. | | | | | | | |  | ● | ● |  |
|  | Include event source, date, username, timestamp, source addresses, destination | | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | addresses, and other useful elements that could assist in a forensic investigation. | | | | | | | |  |  |  |  |
|  |  | 4.9 Log and Alert on Unsuccessful Administrative Account | | | | | | | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |  |  |
| v7 |  | Login | |  |  | |  |  | |  | ● | ● |  |
|  | Configure systems to issue a log entry and alert on unsuccessful logins to an | | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | administrative account. | | | | | | | |  |  |  |  |
| v7 |  | 16.11 Lock Workstation Sessions After Inactivity | | | | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Automatically lock workstation sessions after a standard period of inactivity. | | | | | | | |  |
|  |  |  |  |  |  |
| v7 |  | 16.13 Alert on Account Login Behavior Deviation | | | | | | | |  |  | ● |  |
|  |  | | |  | | |  | |  |  |  |
|  | Alert when users deviate from normal login behavior, such as time-of-day, | | | | | | | |  |  |  |
|  |  | workstation location and duration. | | | | | | | |  |  |  |  |



330 | P a g e

*4.1.8 Ensure session initiation information is collected (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file /var/run/utmp tracks all currently logged in users. All audit records will be tagged with the identifier "session." The /var/log/wtmp file tracks logins, logouts, shutdown, and reboot events. The file /var/log/btmp keeps track of failed login attempts and can be read by entering the command /usr/bin/last -f /var/log/btmp . All audit records will be tagged with the identifier "logins."

*Notes:*

* *The last command can be used to read /var/log/wtmp (last with no parameters)*

*and /var/run/utmp (last -f /var/run/utmp)*

* *Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.*

**Rationale:**

Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).



331 | P a g e

**Audit:**

Run the following commands:

Run the following command and verify rules are in a .rules file:



# grep -E '(session|logins)' /etc/audit/rules.d/\*.rules

Verify output includes:



/etc/audit/rules.d/session.rules:-w /var/run/utmp -p wa -k session

/etc/audit/rules.d/session.rules:-w /var/log/wtmp -p wa -k logins

/etc/audit/rules.d/session.rules:-w /var/log/btmp -p wa -k logins

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep -E '(session|logins)'

Verify output includes:



-w /var/run/utmp -p wa -k session

-w /var/log/wtmp -p wa -k logins

-w /var/log/btmp -p wa -k logins

**Remediation:**

Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

*Example: vi /etc/audit/rules.d/session.rules*

and add the following lines:



-w /var/run/utmp -p wa -k session

-w /var/log/wtmp -p wa -k logins

-w /var/log/btmp -p wa -k logins



332 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 8.5 Collect Detailed Audit Logs | | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Configure detailed audit logging for enterprise assets containing sensitive data. | | | | | | | |  | ● | ● |  |
|  | Include event source, date, username, timestamp, source addresses, destination | | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | addresses, and other useful elements that could assist in a forensic investigation. | | | | | | | |  |  |  |  |
|  |  | 4.9 Log and Alert on Unsuccessful Administrative Account | | | | | | | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |  |  |
| v7 |  | Login | |  |  | |  |  | |  | ● | ● |  |
|  | Configure systems to issue a log entry and alert on unsuccessful logins to an | | | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | administrative account. | | | | | | | |  |  |  |  |
| v7 |  | 16.11 Lock Workstation Sessions After Inactivity | | | | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Automatically lock workstation sessions after a standard period of inactivity. | | | | | | | |  |
|  |  |  |  |  |  |
| v7 |  | 16.13 Alert on Account Login Behavior Deviation | | | | | | | |  |  | ● |  |
|  |  | | |  | | |  | |  |  |  |
|  | Alert when users deviate from normal login behavior, such as time-of-day, | | | | | | | |  |  |  |
|  |  | workstation location and duration. | | | | | | | |  |  |  |  |



333 | P a g e

*4.1.9 Ensure discretionary access control permission modification events are collected (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier "perm\_mod."

*Notes:*

* *Systems may have been customized to change the default UID\_MIN. To confirm the UID\_MIN for your system, run the following command:*
* awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs
* *If your systems' UID\_MIN is not 1000, replace audit>=1000 with audit>=<UID\_MIN for your system> in the Audit and Remediation procedures.*
* *Reloading the auditd config to set active settings may require a system reboot.*

**Rationale:**

Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.



334 | P a g e

**Audit:**

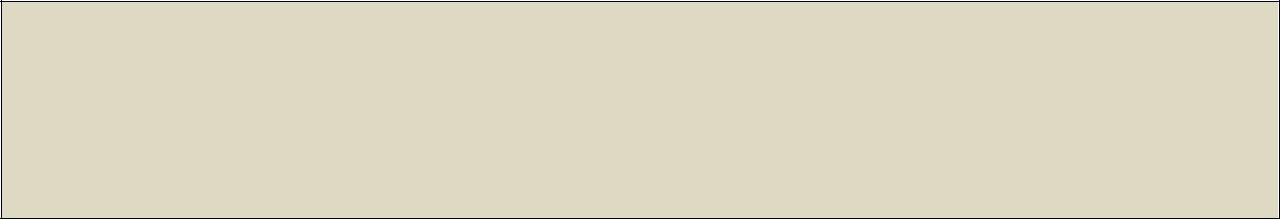
On a 32 bit system run the following commands:

Run the following command and verify rules are in a .rules file:



# grep perm\_mod /etc/audit/rules.d/\*.rules

Verify output matches:



-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm\_mod

-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm\_mod

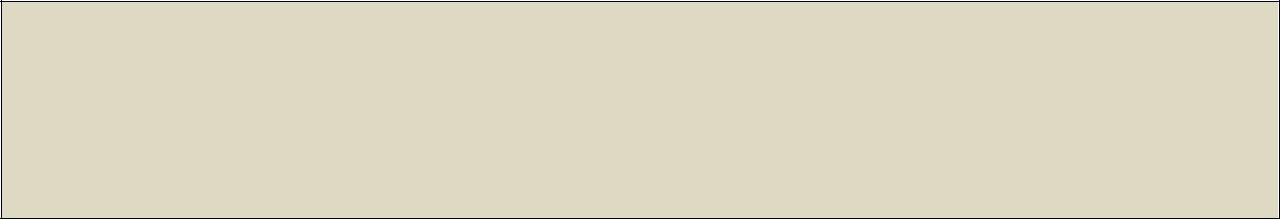
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm\_mod

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep perm\_mod

Verify output matches:



-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm\_mod

-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F auid!=-1 -F key=perm\_mod

-a always,exit -F arch=b32 -S

setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F

auid>=1000 -F auid!=-1 -F key=perm\_mod

On a 64 bit system run the following commands:

Run the following command and verify rules are in a .rules file:

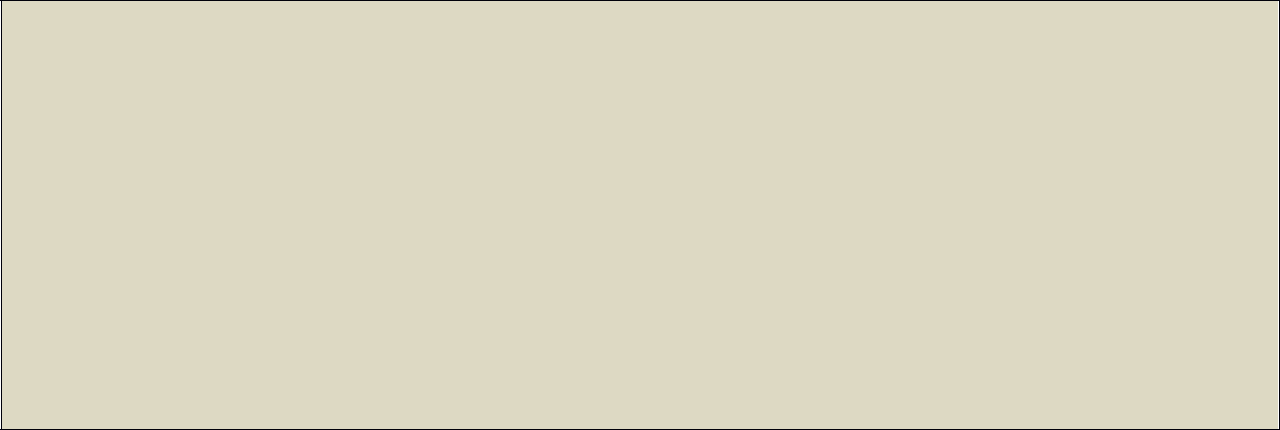


# grep perm\_mod /etc/audit/rules.d/\*.rules



335 | P a g e

Verify output matches:



/etc/audit/rules.d/perm\_mod.rules:-a always,exit -F arch=b64 -S chmod -S

fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm\_mod

/etc/audit/rules.d/perm\_mod.rules:-a always,exit -F arch=b32 -S chmod -S

fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm\_mod

/etc/audit/rules.d/perm\_mod.rules:-a always,exit -F arch=b64 -S chown -S

fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm\_mod

/etc/audit/rules.d/perm\_mod.rules:-a always,exit -F arch=b32 -S chown -S

fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm\_mod

/etc/audit/rules.d/perm\_mod.rules:-a always,exit -F arch=b64 -S setxattr -S

lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F

auid>=1000 -F auid!=4294967295 -k perm\_mod

/etc/audit/rules.d/perm\_mod.rules:-a always,exit -F arch=b32 -S setxattr -S

lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F

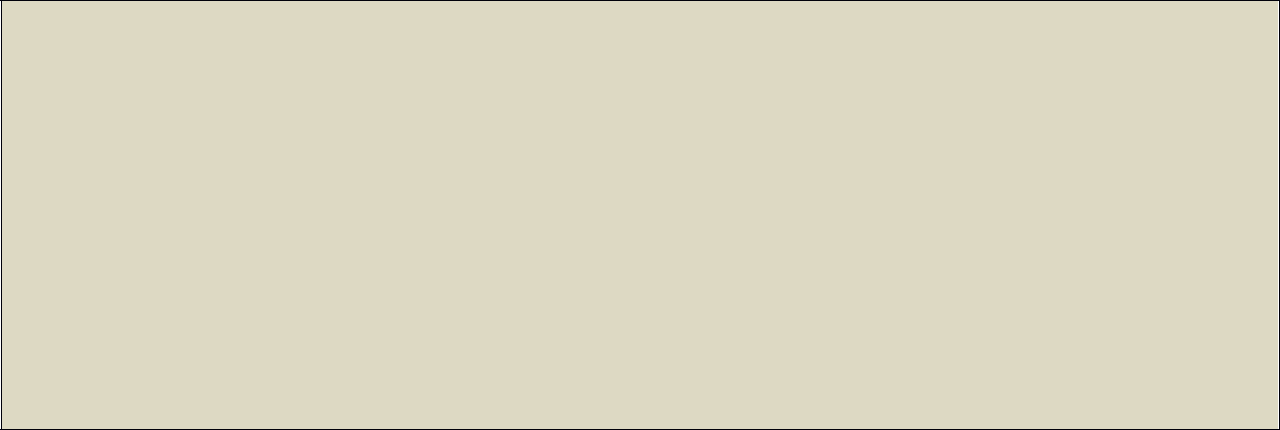
auid>=1000 -F auid!=4294967295 -k perm\_mod

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep perm\_mod

Verify output matches:



-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm\_mod

-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm\_mod

-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F auid!=-1 -F key=perm\_mod

-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F auid!=-1 -F key=perm\_mod

-a always,exit -F arch=b64 -S

setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F

auid>=1000 -F auid!=-1 -F key=perm\_mod

-a always,exit -F arch=b32 -S

setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F

auid>=1000 -F auid!=-1 -F key=perm\_mod



336 | P a g e

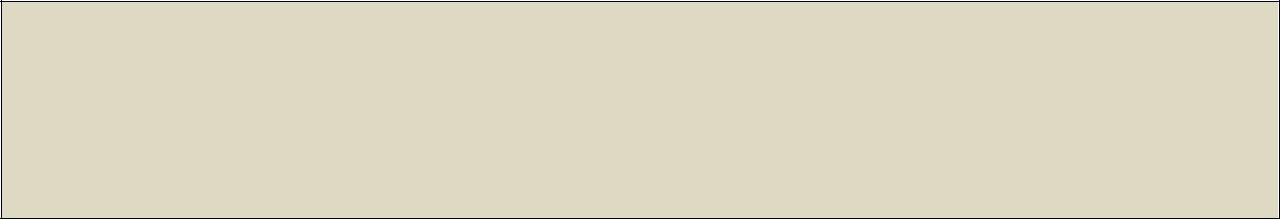
**Remediation:**

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/perm\_mod.rules*

and add the following lines:



-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm\_mod

-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm\_mod

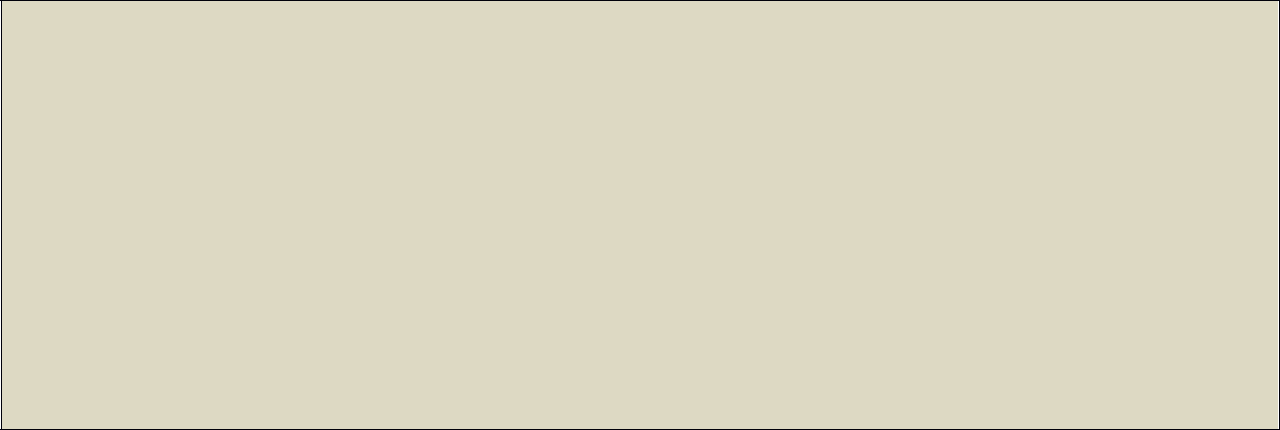
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm\_mod

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/perm\_mod.rules*

and add the following lines:



-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm\_mod

-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm\_mod

-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm\_mod

-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm\_mod

-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm\_mod

-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm\_mod

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 8.5 Collect Detailed Audit Logs | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | 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. | | | |  |  |  |  |
|  | 5.5 Implement Automated Configuration Monitoring Systems | | | |  |  |  |  |
|  |  |  | |  |  |  |  |  |
| v7 | 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. | | | |  |  |  |  |



337 | P a g e

*4.1.10 Ensure unsuccessful unauthorized file access attempts are collected (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation ( creat ), opening ( open , openat ) and truncation ( truncate , ftruncate ) of files. An audit log record will only be written if the user is a non-privileged user (auid > = 1000), is not a Daemon event (auid=4294967295) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier "access."

*Notes:*

* *Systems may have been customized to change the default UID\_MIN. To confirm the UID\_MIN for your system, run the following command:*
* # awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs
* *If your systems' UID\_MIN is not 1000, replace audit>=1000 with audit>=<UID\_MIN for your system> in the Audit and Remediation procedures.*
* *Reloading the auditd config to set active settings may require a system reboot.*

**Rationale:**

Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.



338 | P a g e

**Audit:**

On a 32 bit system run the following commands:

Run the following command and verify rules are in a .rules file:



# grep access /etc/audit/rules.d/\*.rules

Verify output matches:



-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep access

Verify output matches:



-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k access

-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k access

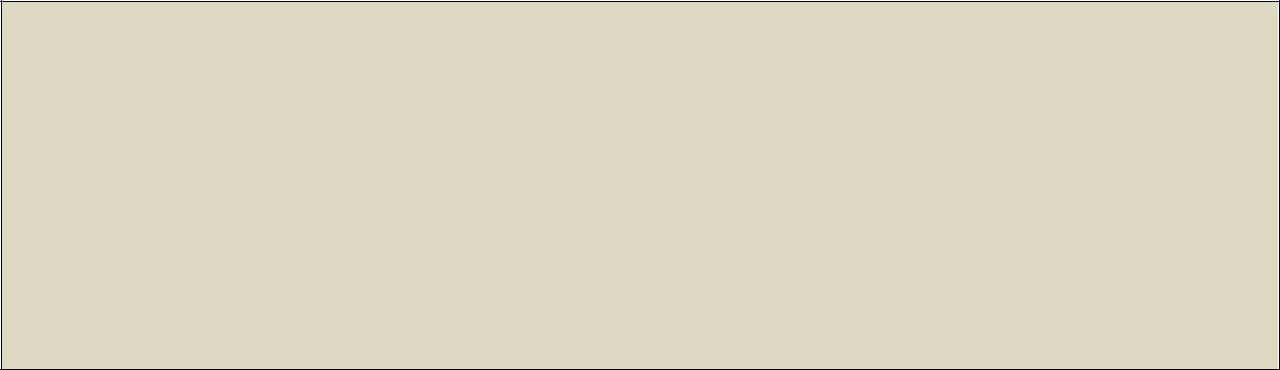
On a 64 bit system run the following commands:

Run the following command and verify rules are in a .rules file:



# grep access /etc/audit/rules.d/\*.rules

Verify output matches:



/etc/audit/rules.d/access.rules:-a always,exit -F arch=b64 -S creat -S open -

1. openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

/etc/audit/rules.d/access.rules:-a always,exit -F arch=b32 -S creat -S open - S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

/etc/audit/rules.d/access.rules:-a always,exit -F arch=b64 -S creat -S open - S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

/etc/audit/rules.d/access.rules:-a always,exit -F arch=b32 -S creat -S open - S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access



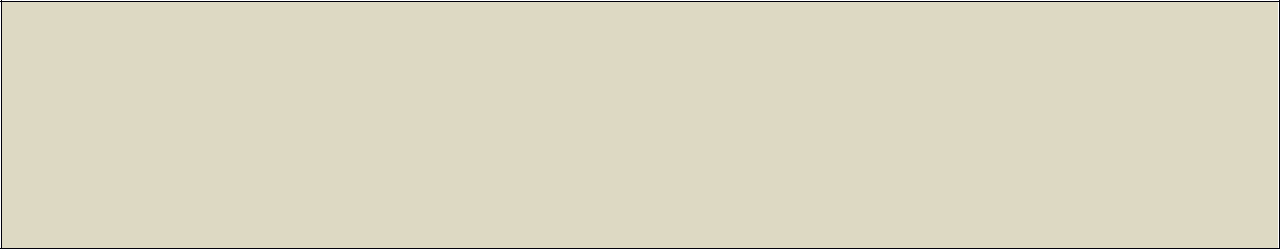
339 | P a g e

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep access

Verify output matches:



-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit=-EACCES -F auid>=1000 -F auid!=-1 -F key=access

-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat -F exit=-EACCES -F auid>=1000 -F auid!=-1 -F key=access

-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit=-EPERM -F auid>=1000 -F auid!=-1 -F key=access

-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat -F exit=-EPERM -F auid>=1000 -F auid!=-1 -F key=access

**Remediation:**

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/access.rules*

and add the following lines:



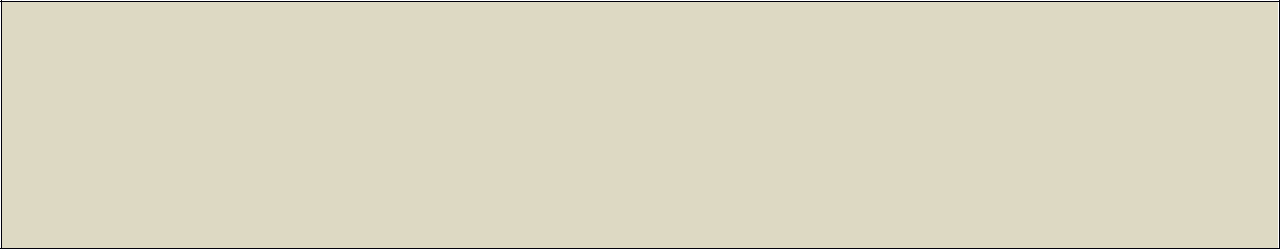
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/access.rules*

and add the following lines:



-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access -a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access



340 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 8.5 Collect Detailed Audit Logs | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | 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. | | | | | |  |  |  |  |
|  |  | 14.9 Enforce Detail Logging for Access or Changes to | | | | | |  |  |  |  |
|  |  |  | |  |  | |  |  |  |  |  |
| v7 |  | Sensitive Data | | |  | | |  |  | ● |  |
|  | Enforce detailed audit logging for access to sensitive data or changes to sensitive | | | | | |  |  |  |
|  |  | data (utilizing tools such as File Integrity Monitoring or Security Information and | | | | | |  |  |  |  |
|  |  | Event Monitoring). | | | | | |  |  |  |  |



341 | P a g e

*4.1.11 Ensure use of privileged commands is collected (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Monitor privileged programs (those that have the setuid and/or setgid bit set on execution) to determine if unprivileged users are running these commands.

*Notes:*

* + *Systems may have been customized to change the default UID\_MIN. To confirm the UID\_MIN for your system, run the following command:*
* awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs
  + *If your systems' UID\_MIN is not 1000, replace audit>=1000 with audit>=<UID\_MIN for your system> in the Audit and Remediation procedures.*
  + *Reloading the auditd config to set active settings may require a system reboot.*



**Rationale:**

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

**Audit:**

Run the following command replacing <partition> with a list of partitions where programs can be executed from on your system:



* find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print "-a always,exit -F path=" $1 " -F perm=x -F auid>='"$(awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs)"' -F auid!=4294967295 -k privileged" }'

Verify all resulting lines are a .rules file in /etc/audit/rules.d/ and the output of

auditctl -l.

*Note: The .rules file output will be auid!=-1 not auid!=4294967295*



342 | P a g e

**Remediation:**

To remediate this issue, the system administrator will have to execute a find command to locate all the privileged programs and then add an audit line for each one of them. The audit parameters associated with this are as follows:

•

-F path=" $1 " - will populate each file name found through the find command and processed by awk.

•

-F perm=x - will write an audit record if the file is executed.

•

-F auid>=1000 - will write a record if the user executing the command is not a privileged user.

•

-F auid!= 4294967295 - will ignore Daemon events

All audit records should be tagged with the identifier "privileged".

Run the following command replacing with a list of partitions where programs can be executed from on your system:



* find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print "-a always,exit -F path=" $1 " -F perm=x -F auid>='"$(awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs)"' -F auid!=4294967295 -k privileged" }'

Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules and add all resulting lines to the file.

*Example:*



* find / -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print "-a always,exit -F path=" $1 " -F perm=x -F auid>='"$(awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs)"' -F auid!=4294967295 -k privileged" }' >> /etc/audit/rules.d/privileged.rules

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |
|  | 8.5 Collect Detailed Audit Logs | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure detailed audit logging for enterprise assets containing sensitive data. | | | |  | ● | ● |  |
| Include event source, date, username, timestamp, source addresses, destination | | | |  |  |
|  |  |  |  |  |
|  | addresses, and other useful elements that could assist in a forensic investigation. | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | ● | ● | ● |  |
|  |  |  |  |  |
| Ensure that local logging has been enabled on all systems and networking devices. | | | |  |
|  |  |  |  |  |



343 | P a g e

*4.1.12 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

*Notes:*

* *Systems may have been customized to change the default UID\_MIN. To confirm the UID\_MIN for your system, run the following command:*
* # awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs
* *If your systems' UID\_MIN is not 1000, replace audit>=1000 with audit>=<UID\_MIN for your system> in the Audit and Remediation procedures.*
* *This tracks successful and unsuccessful mount commands.*
* *File system mounts do not have to come from external media and this action still does not verify write (e.g. CD ROMS).*
* *Reloading the auditd config to set active settings may require a system reboot.*

**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.



344 | P a g e

**Audit:**

On a 32 bit system run the following commands:

Run the following command and verify rules are in a .rules file:



# grep mounts /etc/audit/rules.d/\*.rules

Verify output matches:



-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep mounts

Verify output matches:



-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -k mounts

On a 64 bit system run the following commands:

Run the following command and verify rules are in a .rules file:



# grep mounts /etc/audit/rules.d/\*.rules

Verify output matches:



/etc/audit/rules.d/mounts.rules:-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts /etc/audit/rules.d/mounts.rules:-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep mounts

Verify output matches:



-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=-1 -F key=mounts -a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -F key=mounts



345 | P a g e

**Remediation:**

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/mounts.rules*

and add the following lines:



-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/mounts.rules*

and add the following lines:



-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts

-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |
|  | 8.5 Collect Detailed Audit Logs | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure detailed audit logging for enterprise assets containing sensitive data. | | | |  | ● | ● |  |
| Include event source, date, username, timestamp, source addresses, destination | | | |  |  |
|  |  |  |  |  |
|  | addresses, and other useful elements that could assist in a forensic investigation. | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | ● | ● | ● |  |
|  |  |  |  |  |
| Ensure that local logging has been enabled on all systems and networking devices. | | | |  |
|  |  |  |  |  |



346 | P a g e

*4.1.13 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 following system calls and tags them with the identifier "delete":

* unlink - remove a file
* unlinkat - remove a file attribute
* rename - rename a file
* renameat - rename a file attribute

*Notes:*

* *Systems may have been customized to change the default UID\_MIN. To confirm the UID\_MIN for your system, run the following command:*
* # awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs
* *If your systems' UID\_MIN is not 1000, replace audit>=1000 with audit>=<UID\_MIN for your system> in the Audit and Remediation procedures.*
* *At a minimum, configure the audit system to collect file deletion events for all users and root.*
* *Reloading the auditd config to set active settings may require a system reboot.*

**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.



347 | P a g e

**Audit:**

On a 32 bit system run the following commands:

Run the following command and verify rules are in a .rules file:



# grep delete /etc/audit/rules.d/\*.rules

Verify output matches:



-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep delete

Verify output matches:



-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete

On a 64 bit system run the following commands:

Run the following command and verify rules are in a .rules file:



# grep delete /etc/audit/rules.d/\*.rules

Verify output matches:



/etc/audit/rules.d/deletion.rules:-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete /etc/audit/rules.d/deletion.rules:-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep delete

Verify output matches:



-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F auid>=1000 - F auid!=-1 -F key=delete

-a always,exit -F arch=b32 -S unlink,rename,unlinkat,renameat -F auid>=1000 - F auid!=-1 -F key=delete



348 | P a g e

**Remediation:**

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/deletion.rules*

and add the following lines:



-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/deletion.rules*

and add the following lines:



-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete

-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 8.5 Collect Detailed Audit Logs | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure detailed audit logging for enterprise assets containing sensitive data. | | | | |  | ● | ● |  |
| Include event source, date, username, timestamp, source addresses, destination | | | | |  |  |
|  |  |  |  |  |
|  | addresses, and other useful elements that could assist in a forensic investigation. | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Ensure that local logging has been enabled on all systems and networking devices. | | | | |  |
|  |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



349 | P a g e

*4.1.14 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 a file in the /etc/sudoers.d directory will be written to when the file or its attributes have changed.

*Notes: Reloading the auditd config to set active settings may require a system reboot.*

**Rationale:**

Changes in the /etc/sudoers file, or a file in the /etc/sudoers.d/ directory can indicate that an unauthorized change has been made to scope of system administrator activity.

**Audit:**

Run the following commands:

Run the following command and verify rules are in a .rules file:



# grep scope /etc/audit/rules.d/\*.rules

Verify output matches:



/etc/audit/rules.d/scope.rules:-w /etc/sudoers -p wa -k scope

/etc/audit/rules.d/scope.rules:-w /etc/sudoers.d/ -p wa -k scope

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep scope

Verify output matches:



-w /etc/sudoers -p wa -k scope

-w /etc/sudoers.d -p wa -k scope



350 | P a g e

**Remediation:**

Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

*Example: vi /etc/audit/rules.d/scope.rules*

and add the following lines:



-w /etc/sudoers -p wa -k scope

-w /etc/sudoers.d/ -p wa -k scope

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CIS Controls:** | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 8.5 Collect Detailed Audit Logs | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Configure detailed audit logging for enterprise assets containing sensitive data. | | | | |  | ● | ● |  |
|  | Include event source, date, username, timestamp, source addresses, destination | | | | |  |  |
|  |  |  |  |  |  |
|  |  | addresses, and other useful elements that could assist in a forensic investigation. | | | | |  |  |  |  |
|  |  | 4.8 Log and Alert on Changes to Administrative Group | | | | |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |
| v7 |  | Membership | |  | | |  | ● | ● |  |
|  | Configure systems to issue a log entry and alert when an account is added to or | | | | |  |  |
|  |  |  |  |  |  |
|  |  | removed from any group assigned administrative privileges. | | | | |  |  |  |  |



351 | P a g e

*4.1.15 Ensure system administrator actions (sudolog) are collected (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Monitor the sudo log file. The sudo log file is configured in /etc/sudoers or a file in

/etc/sudoers.d.

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 to the sudo log file. Any time a command is executed, an audit event will be triggered as the sudo log file will be opened for write and the executed administration command will be written to the log.

*Notes:*

* *The system must be configured with su disabled (See Item 5.6 Ensure access to the su command is restricted) to force all command execution through sudo. This will not be effective on the console, as administrators can log in as root.*
* *Reloading the auditd config to set active settings may require a system reboot.*

**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.



352 | P a g e

**Audit:**

Run the following commands:



* grep -E "^\s\*-w\s+$(grep -r logfile /etc/sudoers\* | sed -e 's/.\*logfile=//;s/,? .\*//')\s+-p\s+wa\s+-k\s+actions" /etc/audit/rules.d/\*.rules
* auditctl -l | grep actions

Verify output of both matches the output of the following command, and the the output includes a file path



echo "-w $(grep -r logfile /etc/sudoers\* | sed -e 's/.\*logfile=//;s/,? .\*//') -p wa -k actions"

*Example Output*



-w /var/log/sudo.log -p wa -k actions

**Remediation:**

Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules and add the following line:



-w <Path to sudo logfile> -p wa -k actions

*Example: vi /etc/audit/rules.d/actions.rules*

and add the following line:



-w /var/log/sudo.log -p wa -k actions

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 8.5 Collect Detailed Audit Logs | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Configure detailed audit logging for enterprise assets containing sensitive data. | | | | |  | ● | ● |  |
|  | Include event source, date, username, timestamp, source addresses, destination | | | | |  |  |
|  |  |  |  |  |  |
|  |  | addresses, and other useful elements that could assist in a forensic investigation. | | | | |  |  |  |  |
|  |  | 4.9 Log and Alert on Unsuccessful Administrative Account | | | | |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |
| v7 |  | Login | |  | | |  | ● | ● |  |
|  | Configure systems to issue a log entry and alert on unsuccessful logins to an | | | | |  |  |
|  |  |  |  |  |  |
|  |  | administrative account. | | | | |  |  |  |  |



353 | P a g e

*4.1.16 Ensure kernel module loading and unloading is collected (Automated)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

Monitor the loading and unloading of kernel modules. The programs insmod (install a kernel module), rmmod (remove a kernel module), and modprobe (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The init\_module (load a module) and delete\_module (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of "modules".

*Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.*

**Rationale:**

Monitoring the use of insmod , rmmod and modprobe could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the init\_module and delete\_module system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.



354 | P a g e

**Audit:**

On a 32 bit system run the following commands:

Run the following command and verify rules are in a .rules file:



# grep modules /etc/audit/rules.d/\*.rules

Verify output matches:



-w /sbin/insmod -p x -k modules

-w /sbin/rmmod -p x -k modules

-w /sbin/modprobe -p x -k modules

-a always,exit -F arch=b32 -S init\_module -S delete\_module -k modules

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep modules

Verify output matches:



-w /sbin/insmod -p x -k modules

-w /sbin/rmmod -p x -k modules

-w /sbin/modprobe -p x -k modules

-a always,exit -F arch=b32 -S init\_module,delete\_module -F key=modules

On a 64 bit system run the following commands:

Run the following command and verify rules are in a .rules file:



# grep modules /etc/audit/rules.d/\*.rules

Verify output matches:



/etc/audit/rules.d/modules.rules:-w /sbin/insmod -p x -k modules

/etc/audit/rules.d/modules.rules:-w /sbin/rmmod -p x -k modules

/etc/audit/rules.d/modules.rules:-w /sbin/modprobe -p x -k modules /etc/audit/rules.d/modules.rules:-a always,exit -F arch=b64 -S init\_module -S delete\_module -k modules

Run the following command and verify the rules are in the running auditd config:



# auditctl -l | grep modules

Verify output matches:



-w /sbin/insmod -p x -k modules

-w /sbin/rmmod -p x -k modules

-w /sbin/modprobe -p x -k modules

-a always,exit -F arch=b64 -S init\_module,delete\_module -F key=modules

**Remediation:**



355 | P a g e

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/modules.rules*

and add the following lines:



-w /sbin/insmod -p x -k modules

-w /sbin/rmmod -p x -k modules

-w /sbin/modprobe -p x -k modules

-a always,exit -F arch=b32 -S init\_module -S delete\_module -k modules

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in

.rules

*Example: vi /etc/audit/rules.d/modules.rules*

and add the following lines:



-w /sbin/insmod -p x -k modules

-w /sbin/rmmod -p x -k modules

-w /sbin/modprobe -p x -k modules

-a always,exit -F arch=b64 -S init\_module -S delete\_module -k modules

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 8.5 Collect Detailed Audit Logs | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure detailed audit logging for enterprise assets containing sensitive data. | | | |  | ● | ● |  |
| Include event source, date, username, timestamp, source addresses, destination | | | |  |  |
|  |  |  |  |  |
|  | addresses, and other useful elements that could assist in a forensic investigation. | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | ● | ● | ● |  |
|  |  | |  |  |
| Maintain documented, standard security configuration standards for all authorized | | | |  |
|  | operating systems and software. | | | |  |  |  |  |



356 | P a g e

*4.1.17 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 "^\s\*[^#]" /etc/audit/rules.d/\*.rules | tail -1 -e 2

**Remediation:**

Edit or create the file /etc/audit/rules.d/99-finalize.rules and add the following line at the end of the file:



-e 2



357 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Ensure that local logging has been enabled on all systems and networking devices. | | | | |  |
|  |  |  |  |  |
|  | 6.3 Enable Detailed Logging | | | | |  |  |  |  |
|  |  |  | |  | |  |  |  |  |
| v7 | Enable system logging to include detailed information such as an event source, | | | | |  | ● | ● |  |
| date, user, timestamp, source addresses, destination addresses, and other useful | | | | |  |  |
|  |  |  |  |  |
|  | elements. | | | | |  |  |  |  |



358 | P a g e

***4.2 Configure Logging***

Logging services should be configured to prevent information leaks and to aggregate logs on a remote server so that they can be reviewed in the event of a system compromise and ease log analysis.



359 | P a g e

***4.2.1 Configure rsyslog***

The rsyslog software is recommended as a replacement for the syslogd daemon and provides improvements over syslogd, such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

*Notes:*

* *If another logging software, like syslog-ng, is in use on the system, this section can be skipped. Ensure the logging software is secured in accordance with local site policy and the logging software's recommended security settings*
* *If another logging software like syslog-ng is in use on the system:*

1. *This section may be skipped*
2. *Ensure that logging software is configured in accordance with local site policy*



360 | P a g e

*4.2.1.1 Ensure rsyslog is installed (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The rsyslog software is a recommended replacement to the original syslogd daemon.

rsyslog provides improvements over syslogd, including:

* connection-oriented (i.e. TCP) transmission of logs
* The option to log to database formats
* 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:**

Run the following command to Verify rsyslog is installed:



* rpm -q rsyslog rsyslog-<version>

**Remediation:**

Run the following command to install rsyslog:



# zypper install rsyslog



361 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | 8.2 Collect Audit Logs | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Collect audit logs. Ensure that logging, per the enterprise’s audit log management | | | | |  |
|  | process, has been enabled across enterprise assets. | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | ● | ● | ● |  |
|  |  | |  |  |  |
| Ensure that local logging has been enabled on all systems and networking | | | | |  |
|  | devices. | | | | |  |  |  |  |
|  | 6.3 Enable Detailed Logging | | | | |  |  |  |  |
|  |  |  | | |  |  |  |  |  |
| v7 | Enable system logging to include detailed information such as an event source, | | | | |  | ● | ● |  |
| date, user, timestamp, source addresses, destination addresses, and other useful | | | | |  |  |
|  |  |  |  |  |
|  | elements. | | | | |  |  |  |  |



362 | P a g e

*4.2.1.2 Ensure rsyslog Service is enabled and running (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

rsyslog needs to be enabled and running to perform logging

**Rationale:**

If the rsyslog service is not activated the system may default to the syslogd service or lack logging instead.

**Audit:**

Run one of the following commands to verify rsyslog is enabled:



* systemctl is-enabled rsyslog enabled

Run the following command to verify that rsyslog is running:



* systemctl status rsyslog | grep 'active (running) ' Active: active (running) since <Day date time>

**Remediation:**

Run the following command to enable and start rsyslog:



# systemctl --now enable rsyslog



363 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | 8.2 Collect Audit Logs | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Collect audit logs. Ensure that logging, per the enterprise’s audit log management | | | | |  |
|  | process, has been enabled across enterprise assets. | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | ● | ● | ● |  |
|  |  | |  |  |  |
| Ensure that local logging has been enabled on all systems and networking | | | | |  |
|  | devices. | | | | |  |  |  |  |
|  | 6.3 Enable Detailed Logging | | | | |  |  |  |  |
|  |  |  | | |  |  |  |  |  |
| v7 | Enable system logging to include detailed information such as an event source, | | | | |  | ● | ● |  |
| date, user, timestamp, source addresses, destination addresses, and other useful | | | | |  |  |
|  |  |  |  |  |
|  | elements. | | | | |  |  |  |  |



364 | P a g e

*4.2.1.3 Ensure rsyslog default file permissions configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

rsyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

The $FileCreateMode parameter specifies the file creation mode with which rsyslogd creates new files. If not specified, the value 0644 is used.

*Notes:*

* *The value given must always be a 4-digit octal number, with the initial digit being zero.*
* *This setting can be overridden by a less restrictive setting in any file ending in .conf in*

*the /etc/rsyslog.d/ directory*

**Rationale:**

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

**Audit:**

Run the following command and verify that $FileCreateMode is 0640 or more restrictive:



* grep ^\$FileCreateMode /etc/rsyslog.conf /etc/rsyslog.d/\*.conf $FileCreateMode 0640

Verify that no results return with a less restrictive file mode

**Remediation:**

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/\*.conf files and set $FileCreateMode to

0640 or more restrictive:



$FileCreateMode 0640



365 | P a g e

**References:**

1. See the rsyslog.conf(5) man page for more information.

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | ● | ● | ● |  |
|  |  |  | |  |
| Maintain documented, standard security configuration standards for all | | | |  |
|  | authorized operating systems and software. | | | |  |  |  |  |



366 | P a g e

*4.2.1.4 Ensure logging is configured (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/rsyslog.conf and /etc/rsyslog.d/\*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

**Rationale:**

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

**Audit:**

Review the contents of the /etc/rsyslog.conf and /etc/rsyslog.d/\*.conf files to ensure appropriate logging is set. In addition, run the following command and verify that the log files are logging information:



# ls -l /var/log/

**Remediation:**

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/\*.conf files as

appropriate for your environment:

|  |  |
| --- | --- |
| \*.emerg | :omusrmsg:\* |
| auth,authpriv.\* | /var/log/secure |
| mail.\* | -/var/log/mail |
| mail.info | -/var/log/mail.info |
| mail.warning | -/var/log/mail.warn |
| mail.err | /var/log/mail.err |
| news.crit | -/var/log/news/news.crit |
| news.err | -/var/log/news/news.err |
| news.notice | -/var/log/news/news.notice |
| \*.=warning;\*.=err | -/var/log/warn |
|  |  |
| \*.crit | /var/log/warn |
| \*.\*;mail.none;news.none | -/var/log/messages |
| local0,local1.\* | -/var/log/localmessages |
| local2,local3.\* | -/var/log/localmessages |
| local4,local5.\* | -/var/log/localmessages |
| local6,local7.\* | -/var/log/localmessages |
|  |  |

Run the following command to reload the rsyslogd configuration:



# systemctl restart rsyslog



367 | P a g e

**References:**

1. See the rsyslog.conf(5) man page for more information.

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | 8.2 Collect Audit Logs | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Collect audit logs. Ensure that logging, per the enterprise’s audit log management | | | | |  |
|  | process, has been enabled across enterprise assets. | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | ● | ● | ● |  |
|  |  | |  |  |  |
| Ensure that local logging has been enabled on all systems and networking | | | | |  |
|  | devices. | | | | |  |  |  |  |
|  | 6.3 Enable Detailed Logging | | | | |  |  |  |  |
|  |  |  | | |  |  |  |  |  |
| v7 | Enable system logging to include detailed information such as an event source, | | | | |  | ● | ● |  |
| date, user, timestamp, source addresses, destination addresses, and other useful | | | | |  |  |
|  |  |  |  |  |
|  | elements. | | | | |  |  |  |  |



368 | P a g e

*4.2.1.5 Ensure rsyslog is configured to send logs to a remote log host (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The rsyslog utility supports the ability to send logs it gathers to a remote log host running syslogd(8) or to receive messages from remote hosts, reducing administrative overhead.

*Note: The double "at" sign (@@) directs rsyslog to use TCP to send log messages to the server, which is a more reliable transport mechanism than the default UDP protocol*

**Rationale:**

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

**Audit:**

Review the /etc/rsyslog.conf and /etc/rsyslog.d/\*.conf files and verify that logs are

sent to a central host (where loghost.example.com is the name of your central log host):



* grep "^\*.\*[^I][^I]\*@" /etc/rsyslog.conf /etc/rsyslog.d/\*.conf \*.\* @@loghost.example.com

**Remediation:**

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/\*.conf files and add the following line

(where loghost.example.com is the name of your central log host).



\*.\* @@loghost.example.com

Run the following command to reload the rsyslogd configuration:



# systemctl restart rsyslog

**References:**

1. See the rsyslog.conf(5) man page for more information.



369 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |
| v8 | 8.9 Centralize Audit Logs | | | |  | ● | ● |  |
|  |  |  |  |  |  |
| Centralize, to the extent possible, audit log collection and retention across | | | |  |  |
|  | enterprise assets. | | | |  |  |  |  |
| v7 | 6.6 Deploy SIEM or Log Analytic tool | | | |  | ● | ● |  |
|  |  |  |  |  |  |
| Deploy Security Information and Event Management (SIEM) or log analytic | | | |  |  |
|  | tool for log correlation and analysis. | | | |  |  |  |  |
| v7 | 6.8 Regularly Tune SIEM | | | |  |  | ● |  |
|  |  |  | |  |  |  |
| On a regular basis, tune your SIEM system to better identify actionable events | | | |  |  |  |
|  | and decrease event noise. | | | |  |  |  |  |



370 | P a g e

*4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

By default, rsyslog does not listen for log messages coming in from remote systems. The ModLoad tells rsyslog to load the imtcp.so module so it can listen over a network via TCP. The InputTCPServerRun option instructs rsyslogd to listen on the specified TCP port.

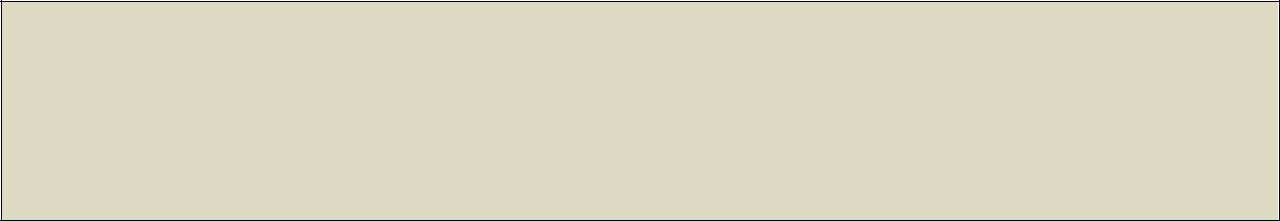
*Note: The $ModLoad imtcp line can have the .so extension added to the end of the module, or use the full path to the module.*

**Rationale:**

The guidance in the section ensures that remote log hosts are configured to only accept rsyslog data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote rsyslog messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

**Audit:**

Run the following commands and verify the resulting lines are uncommitted on designated log hosts and commented or removed on all others:



* grep '$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/\*.conf $ModLoad imtcp
* grep '$InputTCPServerRun' /etc/rsyslog.conf /etc/rsyslog.d/\*.conf $InputTCPServerRun 514

**Remediation:**

For hosts that are designated as log hosts, edit the /etc/rsyslog.conf file and un-comment or add the following lines:



$ModLoad imtcp

$InputTCPServerRun 514

For hosts that are not designated as log hosts, edit the /etc/rsyslog.conf file and comment or remove the following lines:



371 | P a g e

* $ModLoad imtcp
* $InputTCPServerRun 514

Run the following command to reload the rsyslogd configuration:



# systemctl restart rsyslog

**References:**

1. See the rsyslog(8) man page for more information.

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
|  | access control lists, also known as access permissions, to local and remote file | | | | |  |
|  |  |  |  |  |  |
|  |  | systems, databases, and applications. | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |
| v7 |  | Running | |  | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system with | | | | |  |  |
|  |  |  |  |  |  |
|  |  | validated business needs, are running on each system. | | | | |  |  |  |  |



372 | P a g e

***4.2.2 Configure journald***

systemd-journald is a system service that collects and stores logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources: Kernel log messages, via kmsg

Any changes made to the systemd-journald configuration will require a re-start of systemd-journald



373 | P a g e

*4.2.2.1 Ensure journald is configured to send logs to rsyslog (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Data from journald may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of journald logs, however, use of the rsyslog service provides a consistent means of log collection and export.

*Notes:*

* *This recommendation assumes that recommendation 4.2.1.5, "Ensure rsyslog is configured to send logs to a remote log host" has been implemented.*
* *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*
* *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.*

**Rationale:**

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

**Audit:**

Review /etc/systemd/journald.conf and verify that logs are forwarded to syslog



* grep -E ^\s\*ForwardToSyslog /etc/systemd/journald.conf ForwardToSyslog=yes



374 | P a g e

**Remediation:**

Edit the /etc/systemd/journald.conf file and add the following line:



ForwardToSyslog=yes

**References:**

1. [https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsyste](https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf) [mdjournaldconf](https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CIS Controls:** |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| **Controls** |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |
| v8 | 8.9 Centralize Audit Logs | | | |  | ● | ● |  |
|  |  |  |  |  |  |
| Centralize, to the extent possible, audit log collection and retention across | | | |  |  |
|  | enterprise assets. | | | |  |  |  |  |
| v7 | 6.5 Central Log Management | | | |  | ● | ● |  |
|  |  | |  |  |  |
| Ensure that appropriate logs are being aggregated to a central log | | | |  |  |
|  | management system for analysis and review. | | | |  |  |  |  |



375 | P a g e

*4.2.2.2 Ensure journald is configured to compress large log files (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The journald system includes the capability of compressing overly large files to avoid filling up the system with logs or making the log's size unmanageable.

*Note: The main configuration file /etc/systemd/journald.conf is read before any of the custom \*.conf files. If there are custom configs present, they override the main configuration parameters*

**Rationale:**

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

**Audit:**

Review /etc/systemd/journald.conf and verify that large files will be compressed:



* grep -E ^\s\*Compress /etc/systemd/journald.conf Compress=yes

**Remediation:**

Edit the /etc/systemd/journald.conf file and add the following line:



Compress=yes

**References:**

1. [https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsyste](https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf) [mdjournaldconf](https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf)



376 | P a g e

**CIS Controls:**

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



377 | P a g e

*4.2.2.3 Ensure journald is configured to write logfiles to persistent disk (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Data from journald may be stored in volatile memory or persisted locally on the server. Logs in memory will be lost upon a system reboot. By persisting logs to local disk on the server they are protected from loss.

*Note: The main configuration file /etc/systemd/journald.conf is read before any of the custom \*.conf files. If there are custom configs present, they override the main configuration parameters*

**Rationale:**

Writing log data to disk will provide the ability to forensically reconstruct events which may have impacted the operations or security of a system even after a system crash or reboot.

**Audit:**

Review /etc/systemd/journald.conf and verify that logs are persisted to disk:



* grep -E ^\s\*Storage /etc/systemd/journald.conf Storage=persistent

**Remediation:**

Edit the /etc/systemd/journald.conf file and add the following line:



Storage=persistent

**References:**

1. [https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsyste](https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf) [mdjournaldconf](https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf)



378 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | 8.2 Collect Audit Logs | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Collect audit logs. Ensure that logging, per the enterprise’s audit log management | | | | |  |
|  | process, has been enabled across enterprise assets. | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | ● | ● | ● |  |
|  |  | |  |  |  |
| Ensure that local logging has been enabled on all systems and networking | | | | |  |
|  | devices. | | | | |  |  |  |  |
|  | 6.3 Enable Detailed Logging | | | | |  |  |  |  |
|  |  |  | | |  |  |  |  |  |
| v7 | Enable system logging to include detailed information such as an event source, | | | | |  | ● | ● |  |
| date, user, timestamp, source addresses, destination addresses, and other useful | | | | |  |  |
|  |  |  |  |  |
|  | elements. | | | | |  |  |  |  |



379 | P a g e

*4.2.3 Ensure permissions on all logfiles are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well.

**Rationale:**

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected. Other/world should not have the ability to view this information. Group should not have the ability to modify this information.

**Audit:**

Run the following command and verify that other has no permissions on any files and group does not have write or execute permissions on any files:



* find /var/log -type f -perm /g+wx,o+rwx -exec ls -l {} \; Nothing should be returned

**Remediation:**

Run the following commands to set permissions on all existing log files:



find /var/log -type f -exec chmod g-wx,o-rwx "{}" + -o -type d -exec chmod g-wx,o-rwx "{}" +

*Note: The configuration for your logging software or services may need to also be modified for any logs that had incorrect permissions, otherwise, the permissions may be reverted to the incorrect permissions*

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | ● | ● | ● |  |
|  |  |  | |  |
| Maintain documented, standard security configuration standards for all | | | |  |
|  | authorized operating systems and software. | | | |  |  |  |  |



380 | P a g e

*4.2.4 Ensure logrotate is configured (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the log's size unmanageable. The file /etc/logrotate.d/syslog is the configuration file used to rotate log files created by

syslog or rsyslog.

*Note: If no maxage setting is set for logrotate a situation can occur where logrotate is interrupted and fails to delete rotated logfiles. It is recommended to set this to a value greater than the longest any log file should exist on your system to ensure that any such logfile is removed but standard rotation settings are not overridden.*

**Rationale:**

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

**Audit:**

Review /etc/logrotate.conf and /etc/logrotate.d/\* and verify logs are rotated

according to site policy.

**Remediation:**

Edit /etc/logrotate.conf and /etc/logrotate.d/\* to ensure logs are rotated according to site policy.

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

***5 Access, Authentication and Authorization***



381 | P a g e

* Access - Access control for an operating system determines how the operating system implements accesses to system resources by satisfying the security objectives of integrity, availability, and secrecy
* Authentication - Authentication is the process of recognizing a user's identity
* Authorization - Authorization is a security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features



382 | P a g e

***5.1 Configure time-based job schedulers***

cron is a time-based job scheduler used to schedule jobs, commands or shell scripts, to run periodically at fixed times, dates, or intervals.

at provides the ability to execute a command or shell script at a specified date and hour, or after a given interval of time.

Other methods exist for scheduling jobs, such as systemd timers. If another method is used, it should be secured in accordance with local site policy

*Note:* systemd timers *are systemd unit files whose name ends in* .timer *that control* .service *files or events. Timers can be used as an alternative to* cron *and* at*. Timers have* *built-in support for calendar time events, monotonic time events, and can be run asynchronously*

*If cron and at are not installed, this section can be skipped.*



383 | P a g e

*5.1.1 Ensure cron daemon is enabled and running (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The cron daemon is used to execute batch jobs on the system.

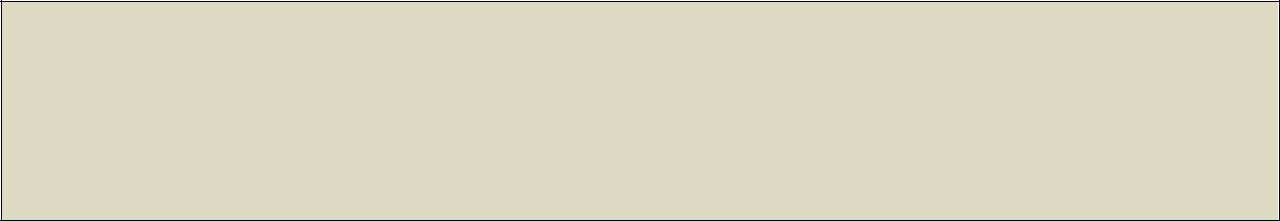
**Rationale:**

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. If another method for scheduling tasks is not being used, cron is used to execute them, and needs to be enabled and running.

**Audit:**

*If cron is installed:*

Run the following commands to verify cron is enabled and running:



* systemctl is-enabled cron enabled
* systemctl status cron | grep 'Active: active (running) ' Active: active (running) since <Day Date Time>

**Remediation:**

Run the following command to enable and start cron:



# systemctl --now enable cron

**CIS Controls:**

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



384 | P a g e

*5.1.2 Ensure permissions on /etc/crontab are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/crontab file is used by cron to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file.

**Rationale:**

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

**Audit:**

*If cron is installed:*

Run the following command and verify Uid and Gid are both 0/root and Access does not grant permissions to group or other:



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # stat /etc/crontab |  |  |  |  |  |  |
| Access: (0600/-rw------- | ) Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |

**Remediation:**

Run the following commands to set ownership and permissions on /etc/crontab:



* chown root:root /etc/crontab
* chmod u-x,og-rwx /etc/crontab

*OR*

Run the following command to remove cron:



# zypper remove cronie



385 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



386 | P a g e

*5.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

This directory contains system cron jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

**Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

**Audit:**

*If cron is installed:*

Run the following command and verify Uid and Gid are both 0/root and Access does not grant permissions to group or other :



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # stat /etc/cron.hourly/ |  |  |  |  |  |  |
| Access: (0700/drwx------ | ) Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |



387 | P a g e

**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/

*OR*

Run the following command to remove cron



# zypper remove cronie

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | ● | ● | ● |  |
|  |  |  | |  |
| Maintain documented, standard security configuration standards for all | | | |  |
|  | authorized operating systems and software. | | | |  |  |  |  |



388 | P a g e

*5.1.4 Ensure permissions on /etc/cron.daily are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/cron.daily directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

**Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

**Audit:**

*If cron is installed:*

Run the following command and verify Uid and Gid are both 0/root and Access does not grant permissions to group or other :



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # stat /etc/cron.daily/ |  |  |  |  |  |  |
| Access: (0700/drwx------ | ) Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |

**Remediation:**

Run the following commands to set ownership and permissions on /etc/cron.daily directory:



* chown root:root /etc/cron.daily
* chmod og-rwx /etc/cron.daily

*OR*

Run the following command to remove cron:



# zypper remove cronie

**CIS Controls:**



389 | P a g e

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



390 | P a g e

*5.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/cron.weekly directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

**Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

**Audit:**

*If cron is installed*

Run the following command and verify Uid and Gid are both 0/root and Access does not grant permissions to group or other :



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # stat /etc/cron.weekly |  |  |  |  |  |  |
| Access: (0700/drwx------ | ) Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |



391 | P a g e

**Remediation:**

Run the following commands to set ownership and permissions on /etc/cron.weekly/ directory:



* chown root:root /etc/cron.weekly/
* chmod og-rwx /etc/cron.weekly/

*OR*

Run the following command to remove cron:



# zypper remove cronie

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



392 | P a g e

*5.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/cron.monthly directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

**Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

**Audit:**

*If cron is installed:*

Run the following command and verify Uid and Gid are both 0/root and Access does not grant permissions to group or other:



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # stat /etc/cron.monthly/ | |  |  |  |  |  |  |
| Access: (0700/drwx------ | ) | Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |



393 | P a g e

**Remediation:**

Run the following commands to set ownership and permissions on /etc/cron.monthly directory:



* chown root:root /etc/cron.monthly
* chmod og-rwx /etc/cron.monthly

*OR*

Run the following command to remove cron:



# zypper remove cronie

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



394 | P a g e

*5.1.7 Ensure permissions on /etc/cron.d are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/cron.d/ directory contains system cron jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from /etc/crontab , but require more granular control as to when they run. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

**Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

**Audit:**

*If cron is installed:*

Run the following command and verify Uid and Gid are both 0/root and Access does not grant permissions to group or other :



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # stat /etc/cron.d |  |  |  |  |  |  |
| Access: (0700/drwx------ | ) Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |

**Remediation:**

Run the following commands to set ownership and permissions on /etc/cron.d directory:



* chown root:root /etc/cron.d
* chmod og-rwx /etc/cron.d

*OR*

Run the following command to remove cron:



# zypper remove cronie

**CIS Controls:**



395 | P a g e

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



396 | P a g e

*5.1.8 Ensure cron is restricted to authorized users (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

If cron is installed in the system, configure /etc/cron.allow to allow specific users to use these services. If /etc/cron.allow does not exist, then /etc/cron.deny is checked. Any user not specifically defined in those files is allowed to use cron. By removing the file, only users in /etc/cron.allow are allowed to use cron.

*Note: Even though a given user is not listed in cron.allow, cron jobs can still be run as that user. The cron.allow file only controls administrative access to the crontab command for scheduling and modifying cron jobs.*

**Rationale:**

On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

**Audit:**

*If cron is installed:*

Run the following command and verify /etc/cron.deny does not exist:



# stat /etc/cron.deny

stat: cannot stat `/etc/cron.deny': No such file or directory

Run the following command and verify Uid and Gid are both 0/root and Access does not

grant permissions to group or other for /etc/cron.allow:



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # stat /etc/cron.allow |  |  |  |  |  |  |
| Access: (0600/-rw------- | ) Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |



397 | P a g e

**Remediation:**

Run the following command to remove /etc/cron.deny:



# rm /etc/cron.deny

Run the following command to create /etc/cron.allow



# touch /etc/cron.allow

Run the following commands to set the owner and permissions on /etc/cron.allow:



* chown root:root /etc/cron.allow
* chmod u-x,og-rwx /etc/cron.allow

*OR*

Run the following command to remove cron



# zypper remove cronie

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | |  |  |  |  |
| v7 | 16 Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |



398 | P a g e

*5.1.9 Ensure at is restricted to authorized users (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

If at is installed in the system, configure /etc/at.allow to allow specific users to use these services. If /etc/at.allow does not exist, then /etc/at.deny is checked. Any user not specifically defined in those files is allowed to use at. By removing the file, only users in /etc/at.allow are allowed to use at.

*Note: Even though a given user is not listed in at.allow, at jobs can still be run as that user. The at.allow file only controls administrative access to the at command for scheduling and modifying at jobs.*

**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:*

Run the following command and verify /etc/at.deny does not exist:



# stat /etc/at.deny

stat: cannot stat `/etc/at.deny': No such file or directory

Run the following command and verify Uid and Gid are both 0/root and Access does not grant permissions to group or other for /etc/at.allow:



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # stat /etc/at.allow |  |  |  |  |  |  |
| Access: (0600/-rw------- | ) Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |



399 | P a g e

**Remediation:**

Run the following command to remove /etc/at.deny:



# rm /etc/at.deny

Run the following command to create /etc/at.allow



# touch /etc/at.allow

Run the following commands to set the owner and permissions on /etc/at.allow:



* chown root:root /etc/at.allow
* chmod u-x,og-rwx /etc/at.allow

*OR*

Run the following command to remove at:



# zypper remove at

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | |  |  |  |  |
| v7 | 16 Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |



400 | P a g e

***5.2 Configure SSH Server***

SSH is a secure, encrypted replacement for common login services such as telnet, ftp, rlogin, rsh, and rcp. It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

*Notes:*

* *The recommendations in this section only apply if the SSH daemon is installed on the system, if remote access is not required the SSH daemon can be removed and this section skipped*
* *Once all configuration changes have been made to /etc/ssh/sshd\_config, the sshd configuration must be reloaded*

Run the following command to reload the sshd configuration:



# systemctl reload sshd



401 | P a g e

*5.2.1 Ensure permissions on /etc/ssh/sshd\_config are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/ssh/sshd\_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root.

**Rationale:**

The /etc/ssh/sshd\_config file needs to be protected from unauthorized changes by non-privileged users.

**Audit:**

Run the following command and verify Uid and Gid are both 0/root and Access does not grant permissions to group or other:



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # stat /etc/ssh/sshd\_config |  |  |  |  |  |
| Access: (0600/-rw-------) Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |

**Remediation:**

Run the following commands to set ownership and permissions on /etc/ssh/sshd\_config:



* chown root:root /etc/ssh/sshd\_config
* chmod og-rwx /etc/ssh/sshd\_config

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



402 | P a g e

*5.2.2 Ensure permissions on SSH private host key files are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

An SSH private key is one of two files used in SSH public key authentication. In this authentication method, The possession of the private key is proof of identity. Only a private key that corresponds to a public key will be able to authenticate successfully. The private keys need to be stored and handled carefully, and no copies of the private key should be distributed.

**Rationale:**

If an unauthorized user obtains the private SSH host key file, the host could be impersonated



403 | P a g e

**Audit:**

*NOTE: Either mode 0640 with owner root and group ssh\_keys OR mode 0600 with owner root and group root is acceptable*

Run the following command and verify either:

Uid is 0/root and Gid is /ssh\_keys and permissions 0640 or more restrictive:

*OR*

Uid is 0/root and Gid is 0/root and permissions are 0600 or more restrictive:



# find /etc/ssh -xdev -type f -name 'ssh\_host\_\*\_key' -exec stat {} \;

*Example Output:*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| File: | ‘/etc/ssh/ssh\_host\_rsa\_key’ | | |  |  |  |  |
| Size: | 1679 | Blocks: 8 | |  | IO Block: 4096 | | regular file |
| Device: | ca01h/51713d | Inode: 8628138 | | | Links: 1 |  |  |
| Access: | (0640/-rw-r-----) | | Uid: ( | 0/ | root) | Gid: ( | 993/ssh\_keys) |
| Access: | 2018-10-22 18:24:56.861750616 +0000 | | | |  |  |  |
| Modify: | 2018-10-22 18:24:56.861750616 +0000 | | | |  |  |  |
| Change: | 2018-10-22 18:24:56.873750616 +0000 | | | |  |  |  |
| Birth: | - |  |  |  |  |  |  |
| File: | ‘/etc/ssh/ssh\_host\_ecdsa\_key’ | | |  |  |  |  |
| Size: | 227 | Blocks: 8 | |  | IO Block: 4096 | | regular file |
| Device: | ca01h/51713d | Inode: 8631760 | | | Links: 1 |  |  |
| Access: | (0640/-rw-r-----) | | Uid: ( | 0/ | root) | Gid: ( | 993/ssh\_keys) |
| Access: | 2018-10-22 18:24:56.897750616 +0000 | | | |  |  |  |
| Modify: | 2018-10-22 18:24:56.897750616 +0000 | | | |  |  |  |
| Change: | 2018-10-22 18:24:56.905750616 +0000 | | | |  |  |  |
| Birth: | - |  |  |  |  |  |  |
| File: | ‘/etc/ssh/ssh\_host\_ed25519\_key’ | | | |  |  |  |
| Size: | 387 | Blocks: 8 | |  | IO Block: 4096 | | regular file |
| Device: | ca01h/51713d | Inode: 8631762 | | | Links: 1 |  |  |
| Access: | (0640/-rw-r-----) | | Uid: ( | 0/ | root) | Gid: ( 993/ssh\_keys) | |
| Access: | 2018-10-22 18:24:56.945750616 +0000 | | | |  |  |  |
| Modify: | 2018-10-22 18:24:56.945750616 +0000 | | | |  |  |  |
| Change: | 2018-10-22 18:24:56.957750616 +0000 | | | |  |  |  |
| Birth: | - |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Remediation:**

Run the following commands to set permissions, ownership, and group on the private SSH host key files:



* find /etc/ssh -xdev -type f -name 'ssh\_host\_\*\_key' -exec chmod u-x,g-wx,o-rwx {} \;
* find /etc/ssh -xdev -type f -name 'ssh\_host\_\*\_key' -exec chown

root:ssh\_keys {} \;

**CIS Controls:**



404 | P a g e

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



405 | P a g e

*5.2.3 Ensure permissions on SSH public host key files are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

An SSH public key is one of two files used in SSH public key authentication. In this authentication method, a public key is a key that can be used for verifying digital signatures generated using a corresponding private key. Only a public key that corresponds to a private key will be able to authenticate successfully.

**Rationale:**

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.



406 | P a g e

**Audit:**

Run the following command and verify Access does not grant write or execute permissions to group or other for all returned files:



# find /etc/ssh -xdev -type f -name 'ssh\_host\_\*\_key.pub' -exec stat {} \;

*Example Output:*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| File: | ‘/etc/ssh/ssh\_host\_rsa\_key.pub’ | | | |  |  |  |  |
| Size: | 382 | Blocks: 8 | |  | IO Block: 4096 | | regular file | |
| Device: | ca01h/51713d | Inode: 8631758 | | | Links: 1 |  |  |  |
| Access: | (0644/-rw-r--r--) | | Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |
| Access: | 2018-10-22 18:24:56.861750616 +0000 | | | |  |  |  |  |
|  |  | | | |  |  |  |  |
| Modify: | 2018-10-22 18:24:56.861750616 +0000 | | | |  |  |  |  |
| Change: | 2018-10-22 18:24:56.881750616 +0000 | | | |  |  |  |  |
| Birth: | - |  |  |  |  |  |  |  |
| File: | ‘/etc/ssh/ssh\_host\_ecdsa\_key.pub’ | | | |  |  |  |  |
| Size: | 162 | Blocks: 8 | |  | IO Block: 4096 | | regular file | |
| Device: | ca01h/51713d | Inode: 8631761 | | | Links: 1 |  |  |  |
| Access: | (0644/-rw-r--r--) | | Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |
| Access: | 2018-10-22 18:24:56.897750616 +0000 | | | |  |  |  |  |
| Modify: | 2018-10-22 18:24:56.897750616 +0000 | | | |  |  |  |  |
| Change: | 2018-10-22 18:24:56.917750616 +0000 | | | |  |  |  |  |
| Birth: | - |  |  |  |  |  |  |  |
| File: | ‘/etc/ssh/ssh\_host\_ed25519\_key.pub’ | | | |  |  |  |  |
| Size: | 82 | Blocks: 8 | |  | IO Block: 4096 | | regular file | |
| Device: | ca01h/51713d | Inode: 8631763 | | | Links: 1 |  |  |  |
| Access: | (0644/-rw-r--r--) | | Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |
| Access: | 2018-10-22 18:24:56.945750616 +0000 | | | |  |  |  |  |
| Modify: | 2018-10-22 18:24:56.945750616 +0000 | | | |  |  |  |  |
| Change: | 2018-10-22 18:24:56.961750616 +0000 | | | |  |  |  |  |
| Birth: | - |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**Remediation:**

Run the following commands to set permissions and ownership on the SSH host public key files



* find /etc/ssh -xdev -type f -name 'ssh\_host\_\*\_key.pub' -exec chmod u-x,go-wx {} \;

#find /etc/ssh -xdev -type f -name 'ssh\_host\_\*\_key.pub' -exec chown root:root {} \;



407 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



408 | P a g e

*5.2.4 Ensure SSH access is limited (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

* AllowUsers:
  1. 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:
  1. 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:
  1. 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:
  1. 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.



409 | P a g e

**Audit:**

Run the following command:



sshd -T | grep -E '^\s\*(allow|deny)(users|groups)\s+\S+'

Verify that the output matches at least one of the following lines:



allowusers <userlist>

allowgroups <grouplist>

denyusers <userlist>

denygroups <grouplist>

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set one or more of the parameter as follows:



AllowUsers <userlist>

*OR*



AllowGroups <grouplist>

*OR*



DenyUsers <userlist>

*OR*



DenyGroups <grouplist>

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 3.3 Configure Data Access Control Lists | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Configure data access control lists based on a user’s need to know. Apply data | | | | | | ● | ● | ● |  |
|  | access control lists, also known as access permissions, to local and remote file | | | | | |  |
|  |  |  |  |  |  |
|  |  | systems, databases, and applications. | | | | | |  |  |  |  |
|  |  | 5.4 Restrict Administrator Privileges to Dedicated | | | | | |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |  |
| v8 |  | Administrator Accounts | |  | | | | ● | ● | ● |  |
|  | Restrict administrator privileges to dedicated administrator accounts on | | | | | |  |
|  |  | enterprise assets. Conduct general computing activities, such as internet browsing, | | | | | |  |  |  |  |
|  |  | email, and productivity suite use, from the user’s primary, non-privileged account. | | | | | |  |  |  |  |
|  |  | 4.3 Ensure the Use of Dedicated Administrative Accounts | | | | | |  |  |  |  |
|  |  |  |  | | | |  |  |  |  |  |
| v7 |  | 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. | | | | | |  |  |  |  |



410 | P a g e

*5.2.5 Ensure SSH LogLevel is appropriate (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

INFO level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

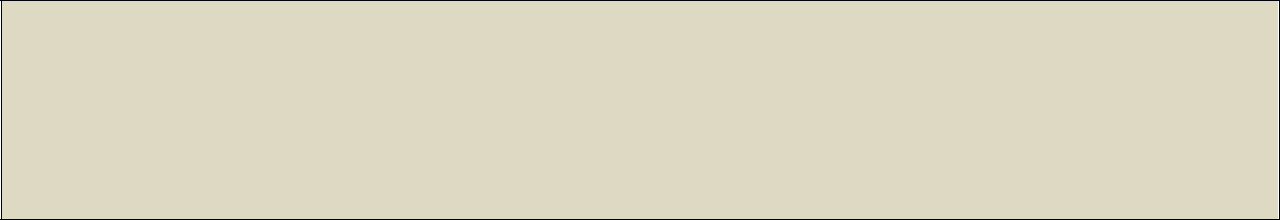
VERBOSE level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments.

**Rationale:**

SSH provides several logging levels with varying amounts of verbosity. DEBUG is specifically **not** recommended other than strictly for debugging SSH communications since it providesso much data that it is difficult to identify important security information.

**Audit:**

Run the following command and verify that output matches:



* sshd -T | grep loglevel loglevel VERBOSE

OR

loglevel INFO

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



LogLevel VERBOSE

*OR*



LogLevel INFO

**Default Value:**

LogLevel INFO

**References:**



411 | P a g e

1. <https://www.ssh.com/ssh/sshd_config/>

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | 8.2 Collect Audit Logs | | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |  |
| Collect audit logs. Ensure that logging, per the enterprise’s audit log management | | | | | |  |
|  | process, has been enabled across enterprise assets. | | | | | |  |  |  |  |
|  | 8.5 Collect Detailed Audit Logs | | | | | |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |
| v8 | Configure detailed audit logging for enterprise assets containing sensitive data. | | | | | |  | ● | ● |  |
| Include event source, date, username, timestamp, source addresses, destination | | | | | |  |  |
|  |  |  |  |  |
|  | addresses, and other useful elements that could assist in a forensic investigation. | | | | | |  |  |  |  |
| v7 | 6.2 Activate audit logging | | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |  |
| Ensure that local logging has been enabled on all systems and networking devices. | | | | | |  |
|  |  |  |  |  |
|  | 6.3 Enable Detailed Logging | | | | | |  |  |  |  |
|  |  |  | | |  | |  |  |  |  |
| v7 | Enable system logging to include detailed information such as an event source, | | | | | |  | ● | ● |  |
| date, user, timestamp, source addresses, destination addresses, and other useful | | | | | |  |  |
|  |  |  |  |  |
|  | elements. | | | | | |  |  |  |  |



412 | P a g e

*5.2.6 Ensure SSH X11 forwarding is disabled (Automated)*

**Profile Applicability:**

* Level 1 - Workstation
* Level 2 - Server

**Description:**

The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.

**Rationale:**

Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

**Audit:**

Run the following command and verify that output matches:



* sshd -T | grep -i x11forwarding x11forwarding no

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



X11Forwarding no

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.8 Uninstall or Disable Unnecessary Services on Enterprise | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Assets and Software | | |  | |  |  | ● | ● |  |
|  | Uninstall or disable unnecessary services on enterprise assets and software, such | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | as an unused file sharing service, web application module, or service function. | | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | | |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |
| v7 |  | Running | |  | | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | with validated business needs, are running on each system. | | | | | |  |  |  |  |



413 | P a g e

*5.2.7 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 | grep maxauthtries maxauthtries 4

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



MaxAuthTries 4

**Default Value:**

MaxAuthTries 6

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 8.5 Collect Detailed Audit Logs | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure detailed audit logging for enterprise assets containing sensitive data. | | | | |  | ● | ● |  |
| Include event source, date, username, timestamp, source addresses, destination | | | | |  |  |
|  |  |  |  |  |
|  | addresses, and other useful elements that could assist in a forensic investigation. | | | | |  |  |  |  |
| v7 | 16.13 Alert on Account Login Behavior Deviation | | | | |  |  | ● |  |
|  | |  | |  |  |  |  |
| Alert when users deviate from normal login behavior, such as time-of-day, | | | | |  |  |  |
|  | workstation location and duration. | | | | |  |  |  |  |



414 | P a g e

*5.2.8 Ensure SSH IgnoreRhosts is enabled (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The IgnoreRhosts parameter specifies that .rhosts and .shosts files will not be used in

RhostsRSAAuthentication or HostbasedAuthentication.

**Rationale:**

Setting this parameter forces users to enter a password when authenticating with ssh.

**Audit:**

Run the following command and verify that output matches:



* sshd -T | grep ignorerhosts ignorerhosts yes

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



IgnoreRhosts yes

**Default Value:**

IgnoreRhosts yes

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 |  | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
|  | and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |  |
|  |  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  |  | Safeguard. | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |
| v7 |  | Running | |  | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system with | | | | |  |  |
|  |  |  |  |  |  |
|  |  | validated business needs, are running on each system. | | | | |  |  |  |  |



415 | P a g e

*5.2.9 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. This option only applies to SSH Protocol Version 2.

**Rationale:**

Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf, disabling the ability to use .rhosts files in SSH provides an additional layer of protection.

**Audit:**

Run the following command and verify that output matches:



* sshd -T | grep hostbasedauthentication hostbasedauthentication no

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



HostbasedAuthentication no

**Default Value:**

HostbasedAuthentication no

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 16.3 Require Multi-factor Authentication | | | | |  | ● | ● |  |
|  | |  |  | |  |  |
| Require multi-factor authentication for all user accounts, on all systems, whether | | | | |  |  |
|  | managed onsite or by a third-party provider. | | | | |  |  |  |  |



416 | P a g e

*5.2.10 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 no.

**Rationale:**

Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via sudo or su. This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

**Audit:**

Run the following command and verify that output matches:



* sshd -T | grep permitrootlogin permitrootlogin no

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



PermitRootLogin no

**Default Value:**

PermitRootLogin without-password

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 5.4 Restrict Administrator Privileges to Dedicated | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 |  | Administrator Accounts | |  | | | ● | ● | ● |  |
|  | Restrict administrator privileges to dedicated administrator accounts on | | | | |  |
|  |  | enterprise assets. Conduct general computing activities, such as internet browsing, | | | | |  |  |  |  |
|  |  | email, and productivity suite use, from the user’s primary, non-privileged account. | | | | |  |  |  |  |
|  |  | 4.3 Ensure the Use of Dedicated Administrative Accounts | | | | |  |  |  |  |
|  |  |  |  | | |  |  |  |  |  |
| v7 |  | 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. | | | | |  |  |  |  |



417 | P a g e

*5.2.11 Ensure SSH PermitEmptyPasswords is disabled (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The PermitEmptyPasswords parameter specifies if the SSH server allows login to accounts with empty password strings.

**Rationale:**

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system

**Audit:**

Run the following command and verify that output matches:



* sshd -T | grep permitemptypasswords permitemptypasswords no

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



PermitEmptyPasswords no

**Default Value:**

PermitEmptyPasswords no

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 16.3 Require Multi-factor Authentication | | | | |  | ● | ● |  |
|  | |  |  | |  |  |
| Require multi-factor authentication for all user accounts, on all systems, whether | | | | |  |  |
|  | managed onsite or by a third-party provider. | | | | |  |  |  |  |



418 | P a g e

*5.2.12 Ensure SSH PermitUserEnvironment is disabled (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The PermitUserEnvironment option allows users to present environment options to the ssh daemon.

**Rationale:**

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has ssh executing a Trojan’s programs)

**Audit:**

Run the following command and verify that output matches:



* sshd -T | grep permituserenvironment permituserenvironment no

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



PermitUserEnvironment no

**Default Value:**

PermitUserEnvironment no

**CIS Controls:**

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



419 | P a g e

*5.2.13 Ensure only strong Ciphers are used (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

This variable limits the ciphers that SSH can use during communication.

*Notes:*

* *Some organizations may have stricter requirements for approved ciphers. Ensure that ciphers used are in compliance with site policy*
* *The only "strong" ciphers currently FIPS 140-2 compliant are: aes256-ctr,aes192-ctr,aes128-ctr*
* *CVE-2013-4548 referenced bellow applies to OpenSSH versions 6.2 and 6.3. If running these versions of Open SSH, Please upgrade to version 6.4 or later to fix the vulnerability, or disable AES-GCM in the server configuration*

The Following are the supported ciphers in openSSH 7.9:



3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

aes128-ctr

aes192-ctr

aes256-ctr

aes128-gcm@openssh.com

aes256-gcm@openssh.com

chacha20-poly1305@openssh.com



420 | P a g e

**Rationale:**

Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised.

* The DES, Triple DES, and Blowfish ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack
* The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue
* The passwords used during an SSH session encrypted with RC4 can be recovered by an attacker who is able to capture and replay the session
* Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors
* The mm\_newkeys\_from\_blob function in monitor\_wrap.c, when an AES-GCM cipher is used, does not properly initialize memory for a MAC context data structure, which allows remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address

**Audit:**

Run the following command and verify that output does not contain any of the listed weak ciphers



# sshd -T | grep ciphers

Weak Ciphers:



3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc



421 | P a g e

**Remediation:**

Edit the /etc/ssh/sshd\_config file add/modify the Ciphers line to contain a comma separated list of the site approved ciphers

Example:



Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

**Default Value:**

Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

**References:**

1. <https://nvd.nist.gov/vuln/detail/CVE-2016-2183>
2. <https://nvd.nist.gov/vuln/detail/CVE-2015-2808>
3. <https://www.kb.cert.org/vuls/id/565052>
4. <https://www.openssh.com/txt/cbc.adv>
5. <https://nvd.nist.gov/vuln/detail/CVE-2008-5161>
6. <https://nvd.nist.gov/vuln/detail/CVE-2013-4548>
7. <https://www.kb.cert.org/vuls/id/565052>
8. <https://www.openssh.com/txt/cbc.adv>
9. SSHD\_CONFIG(5)

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
| v8 | 3.10 Encrypt Sensitive Data in Transit | | | |  | ● | ● |  |
|  |  |  |  |  |  |
| Encrypt sensitive data in transit. Example implementations can include: | | | |  |  |
|  | Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). | | | |  |  |  |  |
| v7 | 14.4 Encrypt All Sensitive Information in Transit | | | |  | ● | ● |  |
|  |  |  |  |  |  |
| Encrypt all sensitive information in transit. | | | |  |  |
|  |  |  |  |  |



422 | P a g e

*5.2.14 Ensure only strong MAC algorithms are used (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

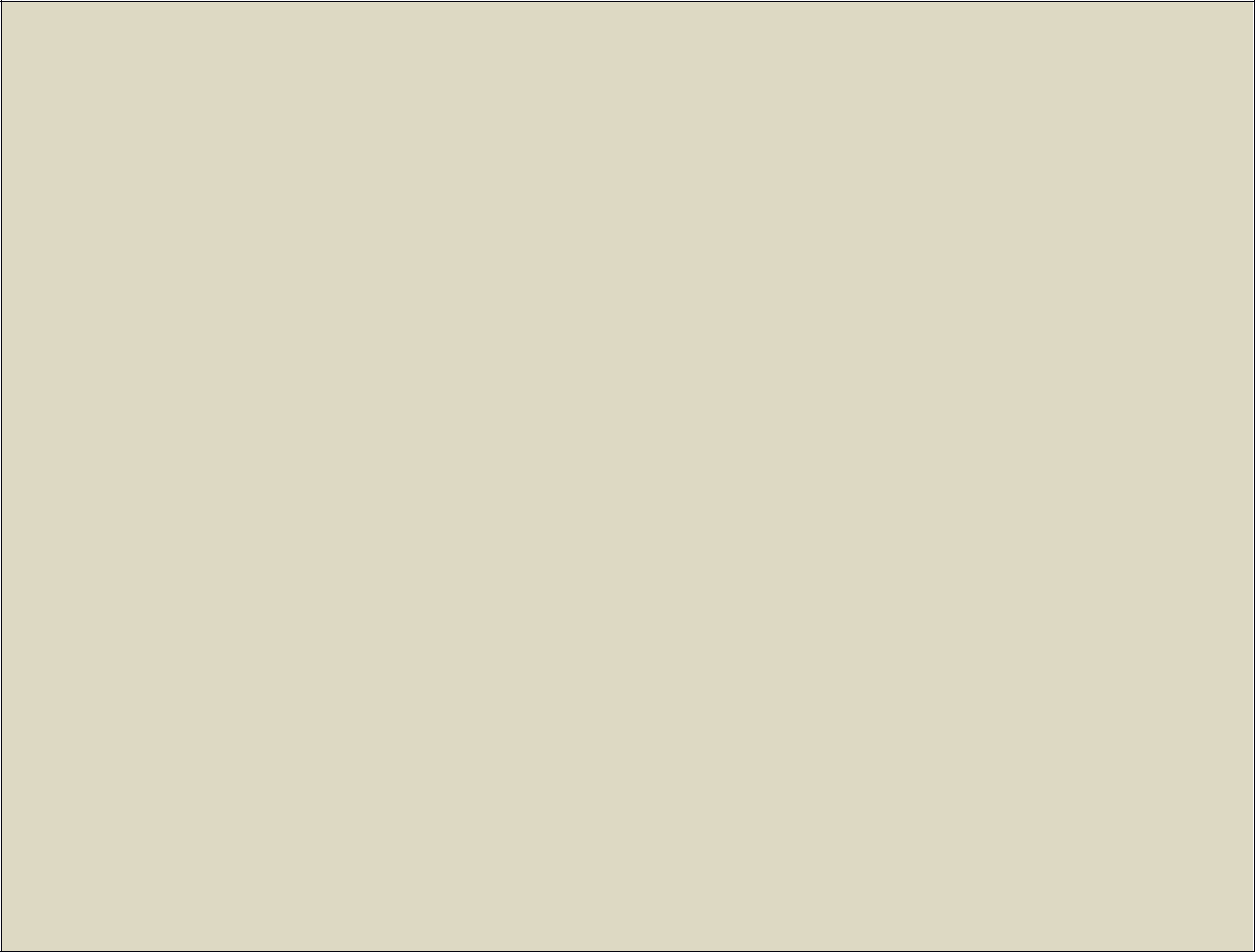
**Description:**

This variable limits the types of MAC algorithms that SSH can use during communication.

*Notes:*

* *Some organizations may have stricter requirements for approved MACs. Ensure that MACs used are in compliance with site policy*
* *The only "strong" MACs currently FIPS 140-2 approved are hmac-sha2-256 and hmac-sha2-512*

The Supported MACs are:



hmac-md5

hmac-md5-96

hmac-sha1

hmac-sha1-96

hmac-sha2-256

hmac-sha2-512

umac-64@openssh.com

umac-128@openssh.com

hmac-md5-etm@openssh.com

hmac-md5-96-etm@openssh.com

hmac-sha1-etm@openssh.com

hmac-sha1-96-etm@openssh.com

hmac-sha2-256-etm@openssh.com

hmac-sha2-512-etm@openssh.com

umac-64-etm@openssh.com

umac-128-etm@openssh.com



423 | P a g e

**Rationale:**

MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information

**Audit:**

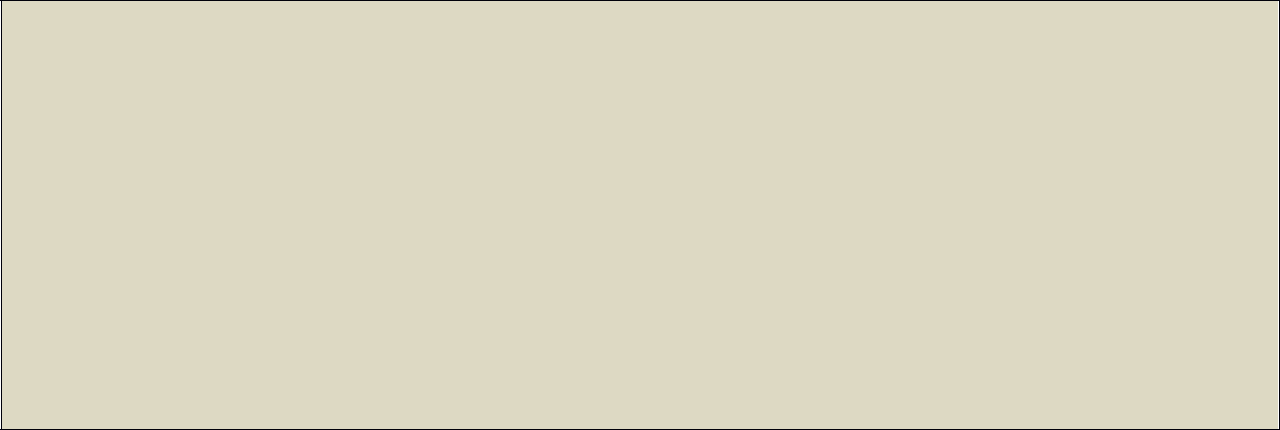
Run the following command and verify that output does not contain any of the listed weak

MAC algorithms:



# sshd -T | grep -i "MACs"

Weak MAC algorithms:



hmac-md5

hmac-md5-96

hmac-ripemd160

hmac-sha1

hmac-sha1-96

umac-64@openssh.com

umac-128@openssh.com

hmac-md5-etm@openssh.com

hmac-md5-96-etm@openssh.com

hmac-ripemd160-etm@openssh.com

hmac-sha1-etm@openssh.com

hmac-sha1-96-etm@openssh.com

umac-64-etm@openssh.com

umac-128-etm@openssh.com

**Remediation:**

Edit the /etc/ssh/sshd\_config file and add/modify the MACs line to contain a comma separated list of the site approved MACs

*Example:*



MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256

**Default Value:**

MACs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1



424 | P a g e

**References:**

1. More information on SSH downgrade attacks can be found here: <http://www.mitls.org/pages/attacks/SLOTH>
2. SSHD\_CONFIG(5)

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.1 Establish and Maintain a Secure Configuration Process | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | | |  |  |  |  |
| v8 |  | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | | ● | ● | ● |  |
|  | and software (operating systems and applications). Review and update documentation | | | | | |  |
|  |  |  |  |  |  |
|  |  | annually, or when significant enterprise changes occur that could impact this | | | | | |  |  |  |  |
|  |  | Safeguard. | | | | | |  |  |  |  |
| v7 |  | 14.4 Encrypt All Sensitive Information in Transit | | | | | |  | ● | ● |  |
|  |  |  |  |  |  |  |  |  |
|  | Encrypt all sensitive information in transit. | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | 16.5 Encrypt Transmittal of Username and Authentication | | | | | |  |  |  |  |
|  |  |  | |  |  | |  |  |  |  |  |
| v7 |  | Credentials | | |  | | |  | ● | ● |  |
|  | Ensure that all account usernames and authentication credentials are transmitted | | | | | |  |  |
|  |  |  |  |  |  |
|  |  | across networks using encrypted channels. | | | | | |  |  |  |  |



425 | P a g e

*5.2.15 Ensure only strong Key Exchange algorithms are used (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

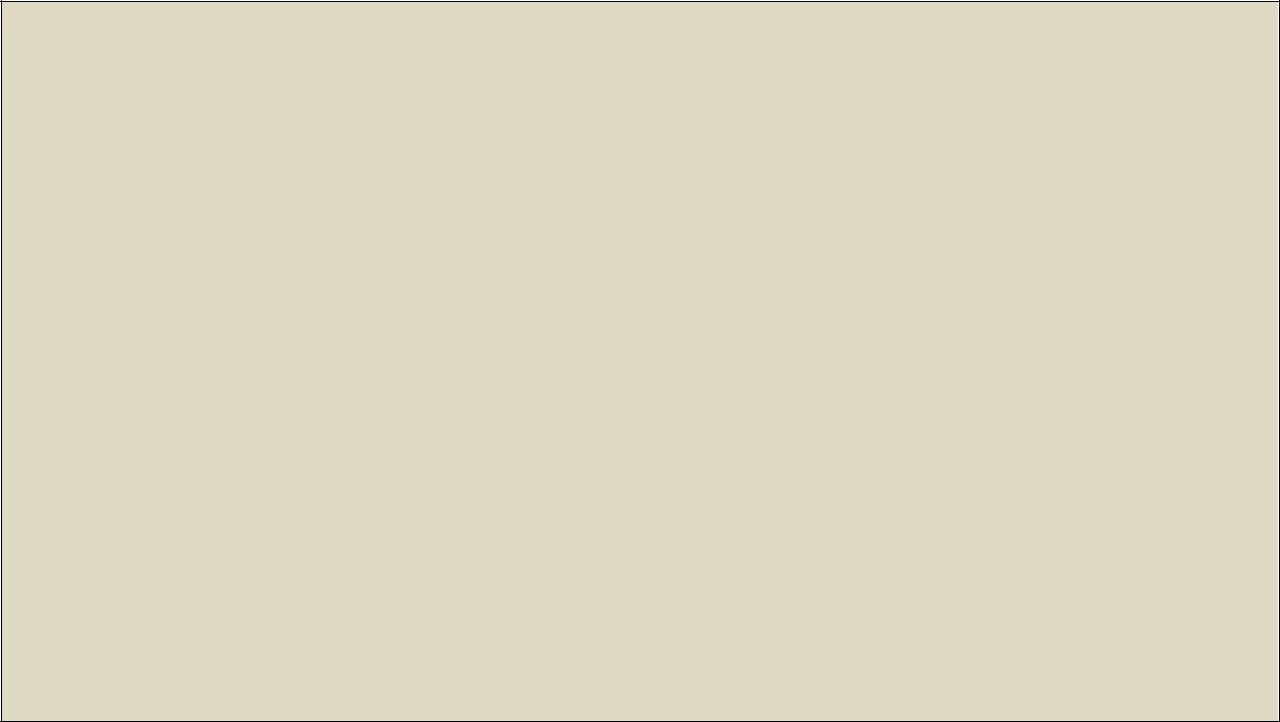
**Description:**

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received

*Notes: Kex algorithms have a higher preference the earlier they appear in the list*

* *Some organizations may have stricter requirements for approved Key exchange algorithms. Ensure that Key exchange algorithms used are in compliance with site policy.*
* *The only Key Exchange Algorithms currently FIPS 140-2 approved are: ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256*

*The Key Exchange algorithms supported by OpenSSH 7.9 are:*



curve25519-sha256

curve25519-sha256@libssh.org

diffie-hellman-group1-sha1

diffie-hellman-group14-sha1

diffie-hellman-group14-sha256

diffie-hellman-group16-sha512

diffie-hellman-group18-sha512

diffie-hellman-group-exchange-sha1

diffie-hellman-group-exchange-sha256

ecdh-sha2-nistp256

ecdh-sha2-nistp384

ecdh-sha2-nistp521



426 | P a g e

**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 | grep kexalgorithms

Weak Key Exchange Algorithms:



diffie-hellman-group1-sha1

diffie-hellman-group14-sha1

diffie-hellman-group-exchange-sha1

**Remediation:**

Edit the /etc/ssh/sshd\_config file add/modify the KexAlgorithms line to contain a comma separated list of the site approved key exchange algorithms

*Example*



KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256

**Default Value:**

KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 14.4 Encrypt All Sensitive Information in Transit | | | | |  | ● | ● |  |
|  |  |  |  |  |  |  |
| Encrypt all sensitive information in transit. | | | | |  |  |
|  |  |  |  |  |



427 | P a g e

*5.2.16 Ensure SSH Idle Timeout Interval is configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The two options ClientAliveInterval and ClientAliveCountMax control the timeout of

ssh sessions.

* ClientAliveInterval sets a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client.
* ClientAliveCountMax sets the number of client alive messages which may be sent without sshd receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. The default value is 3.

o The client alive messages are sent through the encrypted channel o Setting ClientAliveCountMax to 0 disables connection termination

*Example:* If the ClientAliveInterval is set to 15 seconds and the ClientAliveCountMax is

set to 3, the client ssh session will be terminated after 45 seconds of idle time.

**Rationale:**

Having no timeout value associated with a connection could allow an unauthorized user access to another user's ssh session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value reduces this risk.

* The recommended ClientAliveInterval setting is 300 seconds (5 minutes)
* The recommended ClientAliveCountMax setting is 3
* The ssh session would send three keep alive messages at 5 minute intervals. If no response is received after the third keep alive message, the ssh session would be terminated after 15 minutes.



428 | P a g e

**Audit:**

Run the following commands and verify ClientAliveInterval is between 1 and 300:



* sshd -T | grep clientaliveinterval clientaliveinterval 300

Run the following command and verify ClientAliveCountMax is between 1 and 3:



* sshd -T | grep clientalivecountmax clientalivecountmax 3

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameters according to site policy. This

should include ClientAliveInterval between 1 and 300 and ClientAliveCountMax of 3 or

less:



ClientAliveInterval 300

ClientAliveCountMax 3

**Default Value:**

ClientAliveInterval 0

ClientAliveCountMax 3

**References:**

1. <https://man.openbsd.org/sshd_config>

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 16.11 Lock Workstation Sessions After Inactivity | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Automatically lock workstation sessions after a standard period of inactivity. | | | | |  |
|  |  |  |  |  |



429 | P a g e

*5.2.17 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:



* sshd -T | grep logingracetime logingracetime 60

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



LoginGraceTime 60

**Default Value:**

LoginGraceTime 120



430 | P a g e

**CIS Controls:**

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



431 | P a g e

*5.2.18 Ensure SSH warning banner is configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The Banner parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

**Rationale:**

Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

**Audit:**

Run the following command and verify that output matches:



* sshd -T | grep banner banner /etc/issue.net

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



Banner /etc/issue.net

**CIS Controls:**

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



432 | P a g e

*5.2.19 Ensure SSH PAM is enabled (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

UsePAM Enables the Pluggable Authentication Module interface. If set to “yes” this will enable PAM authentication using ChallengeResponseAuthentication and PasswordAuthentication in addition to PAM account and session module processing for all authentication types

**Rationale:**

When usePAM is set to yes, PAM runs through account and session types properly. This is important if you want to restrict access to services based off of IP, time or other factors of the account. Additionally, you can make sure users inherit certain environment variables on login or disallow access to the server

**Impact:**

If UsePAM is enabled, you will not be able to run sshd(8) as a non-root user.

**Audit:**

Run the following command and verify that output matches:



* sshd -T | grep -i usepam usepam yes

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



UsePAM yes

**Default Value:**

usePAM yes



433 | P a g e

**CIS Controls:**

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



434 | P a g e

*5.2.20 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 back-doors.

SSH connections are protected with strong encryption. This makes their contents invisible to most deployed network monitoring and traffic filtering solutions. This invisibility carries considerable risk potential if it is used for malicious purposes such as data exfiltration.

Cybercriminals or malware could exploit SSH to hide their unauthorized communications, or to exfiltrate stolen data from the target network

**Impact:**

SSH tunnels are widely used in many corporate environments that employ mainframe systems as their application backends. In those environments the applications themselves may have very limited native support for security. By utilizing tunneling, compliance with SOX, HIPAA, PCI-DSS, and other standards can be achieved without having to modify the applications.

**Audit:**

Run the following command and verify that output matches:



* sshd -T | grep -i allowtcpforwarding allowtcpforwarding no

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



AllowTcpForwarding no



435 | P a g e

**Default Value:**

AllowTcpForwarding yes

**References:**

1. <https://www.ssh.com/ssh/tunneling/example>

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 |  | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
|  | and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |  |
|  |  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  |  | Safeguard. | | | | |  |  |  |  |
|  |  | 9.2 Ensure Only Approved Ports, Protocols and Services Are | | | | |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |
| v7 |  | Running | |  | | |  | ● | ● |  |
|  | Ensure that only network ports, protocols, and services listening on a system with | | | | |  |  |
|  |  |  |  |  |  |
|  |  | validated business needs, are running on each system. | | | | |  |  |  |  |



436 | P a g e

*5.2.21 Ensure SSH MaxStartups is configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The MaxStartups parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.

**Rationale:**

To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of MaxStartups to protect availability of sshd logins and prevent overwhelming the daemon.

**Audit:**

Run the following command and verify that output MaxStartups is 10:30:60 or matches site policy:



* sshd -T | grep -i maxstartups maxstartups 10:30:60

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



maxstartups 10:30:60

**CIS Controls:**

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



437 | P a g e

*5.2.22 Ensure SSH MaxSessions is limited (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The MaxSessions parameter specifies the maximum number of open sessions permitted 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, or matches site policy:



* sshd -T | grep -i maxsessions maxsessions 10

**Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:



MaxSessions 10

**Default Value:**

MaxSessions 10

**CIS Controls:**

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



438 | P a g e

***5.3 Configure PAM***

PAM (Pluggable Authentication Modules) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the /etc/pam.d directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.



439 | P a g e

*5.3.1 Ensure password creation requirements are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The pam\_cracklib.so module checks the strength of passwords. It performs checks including ensuring a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.

The following are definitions of the pam\_cracklib.so options:

* retry=3 - Allow 3 tries before sending back a failure.
* minlen=14 - password must be 14 characters or more
* 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

Additional module options may be set. This recommendation only covers:

* minlen=
* dcredit=
* ucredit=
* ocredit=
* lcredit=

NOTES: *The settings shown above are one possible policy. If local site policy requires stricter settings, alter these values to conform to your organization's password policies.*

**Rationale:**

Strong passwords and limited attempts before locking an account protect systems from being hacked through brute force methods.



440 | P a g e

pam\_cracklib.so

**Audit:**

Verify password creation requirements conform to organization policy.

Run the following command to verify the minimum password length is at least 14 characters minlen=14:



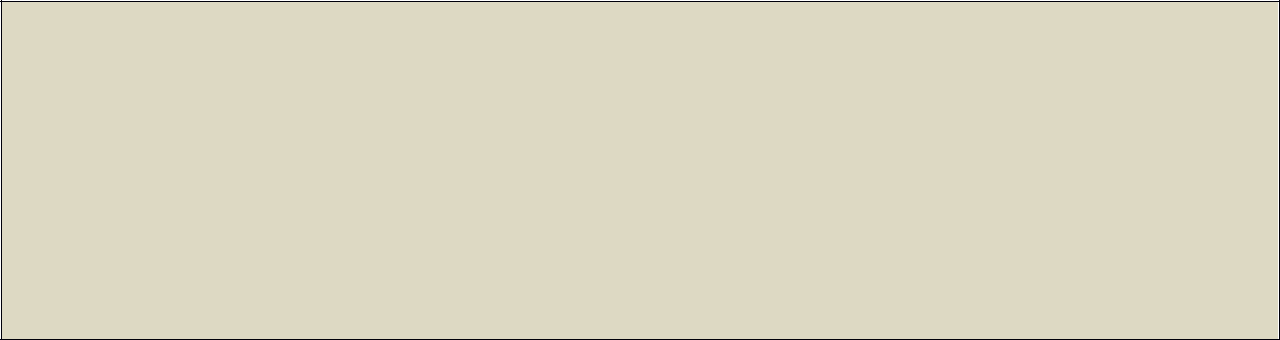
# grep -P

'^\s\*password\s+(requisite|required)\s+pam\_cracklib.so\s+([^#]+\s+)\*minlen=(1 [4-9]|[1-9][0-9]+)\b' /etc/pam.d/common-password

password requisite pam\_cracklib.so retry=3 minlen=14 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1

Run the following command to verify the required password complexity - dcredit=-1

ucredit=-1 ocredit=-1 lcredit=-1:



# grep -P

'^\s\*password\s+(?:requisite|required)\s+pam\_cracklib\.so\s+(?:[^#]+\s+)\*(?:( ?!\2|\3|\4))(dcredit=-[1-9]|ucredit=-[1-9]|ocredit=-[1-9]|lcredit=-[1-9])\s+(?:[^#]+\s+)\*(?:(?!\1|\3|\4))(dcredit=-[1-9]|ucredit=-[1-9]|ocredit=-[1-9]|lcredit=-[1-9])\s+(?:[^#]+\s+)\*(?:(?!\1|\2|\4))(dcredit=-[1-9]|ucredit=-[1-9]|ocredit=-[1-9]|lcredit=-[1-9])\s+(?:[^#]+\s+)\*(?!\1|\2|\3)(dcredit=-[1-9]|ucredit=-[1-9]|ocredit=-[1-9]|lcredit=-[1-9])' /etc/pam.d/common-password

password requisite pam\_cracklib.so retry=3 minlen=14 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1

**Remediation:**

Run the following command:



* pam-config -a --cracklib-minlen=14 --cracklib-retry=3 --cracklib-lcredit=-1 --cracklib-ucredit=-1 --cracklib-dcredit=-1 --cracklib-ocredit=-1 --cracklib

*OR*

Edit the /etc/pam.d/common-password file to include the appropriate options for

and to conform to site policy:



password requisite pam\_cracklib.so retry=3 minlen=14 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1

**References:**

1. <https://documentation.suse.com/sles/15-SP1/html/SLES-all/cha-security-protection.html#sec-sec-prot-general-pam>



441 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |
|  | 5.2 Use Unique Passwords | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| v8 | Use unique passwords for all enterprise assets. Best practice implementation | | | ● | ● | ● |  |
| includes, at a minimum, an 8-character password for accounts using MFA and a 14- | | |  |
|  |  |  |  |  |
|  | character password for accounts not using MFA. | | |  |  |  |  |
| v7 | 4.4 Use Unique Passwords | | |  | ● | ● |  |
|  |  |  |  |  |
| Where multi-factor authentication is not supported (such as local administrator, | | |  |  |
|  | root, or service accounts), accounts will use passwords that are unique to that system. | | |  |  |  |  |



442 | P a g e

deny=\_n\_

*5.3.2 Ensure lockout for failed password attempts is configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Lock out users after *n* unsuccessful consecutive login attempts.

These settings are commonly configured with the pam\_faillock.so module. Some environments may continue using the pam\_tally2.so module, where this older method may simplify automation in mixed environments.

Set the lockout number in deny= to the policy in effect at your site.

unlock\_time=\_n\_ is the number of seconds the account remains locked after the number of

attempts configured in has been met.

*Notes:*

* *Additional module options may be set, recommendation only covers those listed here.*
* *If you want to require the administrator to unlock accounts, leave off the unlock\_time option*
* *The default location for attempted accesses is recorded in /var/log/tallylog*
* *Use of the "audit" keyword may log credentials in the case of user error during authentication. This risk should be evaluated in the context of the site policies of your organization.*
* *You may also lock out root, this should be considered carefully due to the ability to have this setting lock all access to the system*

1. *As an option on the same line:*
   1. auth required pam\_tally2.so deny=5 even\_deny\_root unlock\_time=900
   2. *To define a different lockout time for root:*

o auth required pam\_tally2.so deny=5 root\_unlock\_time=120 unlock\_time=900

* *If a user has been locked out because they have reached the maximum consecutive failure count defined by deny= in the pam\_tally2.so module, the user can be unlocked by issuing following command. This command sets the failed count to 0, effectively unlocking the user.*
* # pam\_tally2 -u <username> --reset

**Rationale:**

Locking out user IDs after *n* unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.



443 | P a g e

**Audit:**

Verify password lockouts are configured. Ensure that the deny=\_n\_ follows local site policy.

This should not exceed deny=5.

Run the following commands:



# grep -E '^\s\*auth\s+\S+\s+pam\_(tally2|unix)\.so' /etc/pam.d/login

Verify the output includes the following lines:



|  |  |  |
| --- | --- | --- |
| auth | required | pam\_tally2.so deny=5 onerr=fail unlock\_time=900 |
| auth | required | pam\_unix.so try\_first\_pass |
|  |  |  |

* grep -E '^\s\*account\s+required\s+pam\_tally2.so\s\*' /etc/pam.d/common-account

Verify the output includes the following lines:



account required pam\_tally2.so

**Remediation:**

Modify the deny= and unlock\_time= parameters to conform to local site policy, Not to be greater than deny=5:

Edit the file /etc/pam.d/login and add the following line:



auth required pam\_tally2.so deny=5 onerr=fail unlock\_time=900

*Note: The ordering on the lines is important. The additional line needs to below the line auth required pam\_env.so and above all password validation lines.*

*Example:*

|  |  |  |
| --- | --- | --- |
| auth | required | pam\_env.so |
| auth | required | pam\_tally2.so deny=5 onerr=fail unlock\_time=900 |
| auth | sufficient | pam\_unix.so nullok try\_first\_pass |
| auth | required | pam\_deny.so |
|  |  |  |

Edit the /etc/pam.d/common-account file and add the following pam\_tally2.so line:



account required pam\_tally2.so



444 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
|  | 16.7 Establish Process for Revoking Access | | | | |  |  |  |  |
|  |  | |  |  | |  |  |  |  |
| v7 | 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. | | | | |  |  |  |  |



445 | P a g e

*5.3.3 Ensure password reuse is limited (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/security/opasswd file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

*Notes:*

* *Additional module options may be set, recommendation only covers those listed here.*
* *This setting only applies to local accounts.*
* *This option is configured with the remember=n module option in /etc/pam.d/common-*

*password*

**Rationale:**

Forcing users not to reuse their past passwords make it less likely that an attacker will be able to guess the password.

**Audit:**

Run the following command to verify remembered password history follows local site policy, not to be less than 5:



# grep -P

'^\s\*password\s+(requisite|required)\s+pam\_pwhistory\.so\s+([^#]+\s+)\*remembe r=([5-9]|[1-9][0-9]+)\b' /etc/pam.d/common-password

password required pam\_pwhistory.so remember=5

**Remediation:**

Run the following command:



# pam-config -a --pwhistory --pwhistory-remember=5

*OR*

Edit the file /etc/pam.d/common-password to include the remember= option and conform to site policy as shown:



password required pam\_pwhistory.so remember=5



446 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |
|  | 5.2 Use Unique Passwords | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Use unique passwords for all enterprise assets. Best practice implementation | | | | ● | ● | ● |  |
| includes, at a minimum, an 8-character password for accounts using MFA and a 14- | | | |  |
|  |  |  |  |  |
|  | character password for accounts not using MFA. | | | |  |  |  |  |
| v7 | 16 Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |



447 | P a g e

***5.4 User Accounts and Environment***

This section provides guidance on setting up secure defaults for system and user accounts and their environment.



448 | P a g e

***5.4.1 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.



449 | P a g e

*5.4.1.1 Ensure password hashing algorithm is SHA-512 (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Login passwords are hashed and stored in the /etc/shadow file.

Note: *These changes only apply to accounts configured on the local system.*

**Rationale:**

The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

**Audit:**

Run the following command to verify the sha512 option is included:



* grep -Ei '^\s\*^\s\*ENCRYPT\_METHOD\s+SHA512' /etc/login.defs ENCRYPT\_METHOD SHA512

**Remediation:**

Edit the /etc/login.defs file and modify ENCRYPT\_METHOD to SHA512:



ENCRYPT\_METHOD sha512

*Notes:*

•

*Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems*

•

*If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login, In accordance with local site policies*

•

*To accomplish this, the following command can be used*



* awk -F: '( $3<'"$(awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs)"' && $1 != "nfsnobody" ) { print $1 }' /etc/passwd | xargs -n 1 chage -d 0



450 | P a g e

**Default Value:**

ENCRYPT\_METHOD sha512

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 3.11 Encrypt Sensitive Data at Rest | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | Encrypt sensitive data at rest on servers, applications, and databases containing | | | |  |  |  |  |
| v8 | sensitive data. Storage-layer encryption, also known as server-side encryption, meets | | | |  | ● | ● |  |
| the minimum requirement of this Safeguard. Additional encryption methods may | | | |  |  |
|  |  |  |  |  |
|  | include application-layer encryption, also known as client-side encryption, where | | | |  |  |  |  |
|  | access to the data storage device(s) does not permit access to the plain-text data. | | | |  |  |  |  |
| v7 | 16.4 Encrypt or Hash all Authentication Credentials | | | |  | ● | ● |  |
|  |  |  |  |  |  |
| Encrypt or hash with a salt all authentication credentials when stored. | | | |  |  |
|  |  |  |  |  |



451 | P a g e

*5.4.1.2 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. It is recommended that the PASS\_MAX\_DAYS parameter be set to less than or equal to 365 days.***

***Notes:***

***• 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.***

***Rationale:***

***The window of opportunity for an attacker to leverage compromised credentials via a brute force attack, using already compromised credentials, or gaining the credentials by other means, can be limited by the age of the password. Therefore, reducing the maximum age of a password can also reduce an attacker's window of opportunity.***

***Requiring passwords to be changed helps to mitigate the risk posed by the poor security practice of passwords being used for multiple accounts, and poorly implemented off-boarding and change of responsibility policies. This should not be considered a replacement for proper implementation of these policies and practices.***

***Note: If it is believed that a user's password may have been compromised, the user's account should be locked immediately. Local policy should be followed to ensure the secure update of their password.***

***452 | P a g e***

******

**Audit:**

Run the following command and verify PASS\_MAX\_DAYS conforms to site policy (no more than 365 days):



* grep ^\s\*PASS\_MAX\_DAYS /etc/login.defs PASS\_MAX\_DAYS 365

Run the following command and Review list of users and PASS\_MAX\_DAYS to verify that all users' PASS\_MAX\_DAYS conforms to site policy (no more than 365 days):



* grep -E '^[^:]+:[^!\*]' /etc/shadow | cut -d: -f1,5 <user>:<PASS\_MAX\_DAYS>

**Remediation:**

Set the PASS\_MAX\_DAYS parameter to conform to site policy in /etc/login.defs :



PASS\_MAX\_DAYS 365

Modify user parameters for all users with a password set to match:



# chage --maxdays 365 <user>

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | |  |  |  |  |
|  | Safeguard. | | | |  |  |  |  |
| v7 | 4.4 Use Unique Passwords | | | |  | ● | ● |  |
|  |  |  | |  |  |
| Where multi-factor authentication is not supported (such as local administrator, | | | |  |  |
|  | root, or service accounts), accounts will use passwords that are unique to that system. | | | |  |  |  |  |



453 | P a g e

*5.4.1.3 Ensure minimum days between password changes is configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The PASS\_MIN\_DAYS parameter in /etc/login.defs allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that PASS\_MIN\_DAYS parameter be set to 1 or more days.

**Rationale:**

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

**Audit:**

Run the following command and verify PASS\_MIN\_DAYS conforms to site policy (no less than 1 day):



* grep ^\s\*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):



* grep -E ^[^:]+:[^\!\*] /etc/shadow | cut -d: -f1,4 <user>:<PASS\_MIN\_DAYS>

**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>



454 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | |  |  |  |  |
|  | Safeguard. | | | |  |  |  |  |
| v7 | 4.4 Use Unique Passwords | | | |  | ● | ● |  |
|  |  |  | |  |  |
| Where multi-factor authentication is not supported (such as local administrator, | | | |  |  |
|  | root, or service accounts), accounts will use passwords that are unique to that system. | | | |  |  |  |  |



455 | P a g e

**Audit:**

**Run the following command and verify**

**7 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.**

**PASS\_WARN\_AGE**

*5.4.1.4 Ensure password expiration warning days is 7 or more (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The PASS\_WARN\_AGE parameter in /etc/login.defs allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the

parameter be set to 7 or more days.

PASS\_WARN\_AGE conforms to site policy (No less than

****

* grep ^\s\*PASS\_WARN\_AGE /etc/login.defs PASS\_WARN\_AGE 7

Verify all users with a password have their number of days of warning before password expires set to 7 or more:

Run the following command and Review list of users and PASS\_WARN\_AGE to verify that all users' PASS\_WARN\_AGE conforms to site policy (No less than 7 days):

****

* grep -E ^[^:]+:[^\!\*] /etc/shadow | cut -d: -f1,6 <user>:<PASS\_WARN\_AGE>

**Remediation:**

Set the PASS\_WARN\_AGE parameter to 7 in /etc/login.defs :

****

PASS\_WARN\_AGE 7

Modify user parameters for all users with a password set to match:

****

# chage --warndays 7 <user>

****

456 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | |  |  |  |  |
|  | Safeguard. | | | |  |  |  |  |
| v7 | 4.4 Use Unique Passwords | | | |  | ● | ● |  |
|  |  |  | |  |  |
| Where multi-factor authentication is not supported (such as local administrator, | | | |  |  |
|  | root, or service accounts), accounts will use passwords that are unique to that system. | | | |  |  |  |  |



457 | P a g e

*5.4.1.5 Ensure inactive password lock is 30 days or less (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

*Note: A value of -1 would disable this setting.*

**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 sire policy (no more than 30 days):



* useradd -D | grep INACTIVE INACTIVE=30

Verify all users with a password have Password inactive no more than 30 days after password expires:

Run the following command and Review list of users and INACTIVE to verify that all users'

INACTIVE conforms to site policy (no more than 30 days):



* grep -E ^[^:]+:[^\!\*] /etc/shadow | cut -d: -f1,7 <user>:<INACTIVE>

**Remediation:**

Run the following command to set the default password inactivity period to 30 days:



# useradd -D -f 30

Modify user parameters for all users with a password set to match:



# chage --inactive 30 <user>



458 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 16.9 Disable Dormant Accounts | | | | | ● | ● | ● |  |
|  |  |  |  |  |  |
| Automatically disable dormant accounts after a set period of inactivity. | | | | |  |
|  |  |  |  |  |



459 | P a g e

*5.4.1.6 Ensure all users last password change date is in the past (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

All users should have a password change date in the past.

**Rationale:**

If a users recorded password change date is in the future then they could bypass any set password expiration.

**Audit:**

Run the following command and verify nothing is returned:



* for usr in $(cut -d: -f1 /etc/shadow); do [[ $(chage --list $usr | grep '^Last password change' | cut -d: -f2) > $(date) ]] && echo "$usr :$(chage -- list $usr | grep '^Last password change' | cut -d: -f2)"; done

**Remediation:**

Investigate any users with a password change date in the future and correct them. Locking the account, expiring the password, or resetting the password manually may be appropriate.

**CIS Controls:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |
|  | 5.2 Use Unique Passwords | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| v8 | Use unique passwords for all enterprise assets. Best practice implementation | | | ● | ● | ● |  |
| includes, at a minimum, an 8-character password for accounts using MFA and a 14- | | |  |
|  |  |  |  |  |
|  | character password for accounts not using MFA. | | |  |  |  |  |
| v7 | 4.4 Use Unique Passwords | | |  | ● | ● |  |
|  |  |  |  |  |
| Where multi-factor authentication is not supported (such as local administrator, | | |  |  |
|  | root, or service accounts), accounts will use passwords that are unique to that system. | | |  |  |  |  |



460 | P a g e

*5.4.2 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.

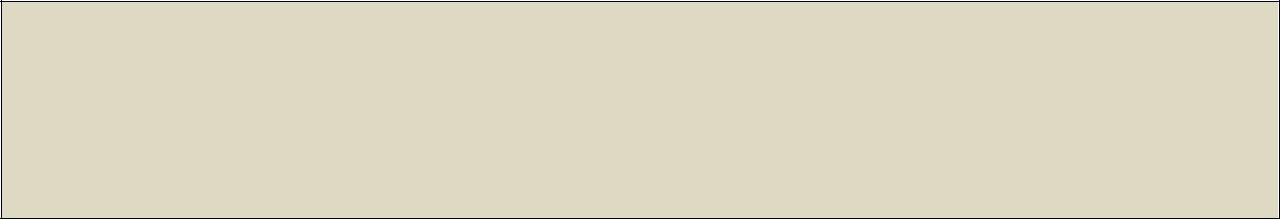
**Rationale:**

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.

*Note: The root, sync, shutdown, and halt users are exempted from requiring a non-login shell.*

**Audit:**

Run the following commands and verify no results are returned:



* awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $1!~/^\+/ && $3<'"$(awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs)"' && $7!="'"$(which nologin)"'" && $7!="/bin/false") {print}' /etc/passwd
* awk -F: '($1!="root" && $1!~/^\+/ && $3<'"$(awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' | awk '($2!="L" && $2!="LK") {print $1}'



461 | P a g e

**Remediation:**

Run the commands appropriate for your distribution:

Set the shell for any accounts returned by the audit to nologin:



# usermod -s $(which nologin) <user>

Lock any non root accounts returned by the audit:



# usermod -L <user>

The following command will set all system accounts to a non login shell:



* awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $1!~/^\+/ && $3<'"$(awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs)"' && $7!="'"$(which nologin)"'" && $7!="/bin/false" && $7!="/usr/bin/false") {print $1}' /etc/passwd | while read -r user; do usermod -s "$(which nologin)" "$user"; done

The following command will automatically lock not root system accounts:



* awk -F: '($1!="root" && $1!~/^\+/ && $3<'"$(awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' | awk '($2!="L" && $2!="LK") {print $1}' | while read -r user; do usermod -L "$user"; done

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | |  |  |  |  |
| v7 | 16 Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |



462 | P a g e

*5.4.3 Ensure default group for the root account is GID 0 (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The usermod command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.

**Rationale:**

Using GID 0 for the root account helps prevent root -owned files from accidentally becoming accessible to non-privileged users.

**Audit:**

Run the following command and verify the result is 0 :



* grep "^root:" /etc/passwd | cut -f4 -d:

0

**Remediation:**

Run the following command to set the root user default group to GID 0 :



# usermod -g 0 root

**CIS Controls:**

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



463 | P a g e

**BASH\_ENV**

*5.4.4 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 .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** **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.

*Notes:*

* 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 for other shells not covered here.
* The TMOUT option applies to the active shell only. In case a user switches from one shell to another, it needs another full cycle to close the remaining shell.
* /etc/profile may get updated by YaST2 Online Update
* Ensure that the timeout conforms to your local policy.

****

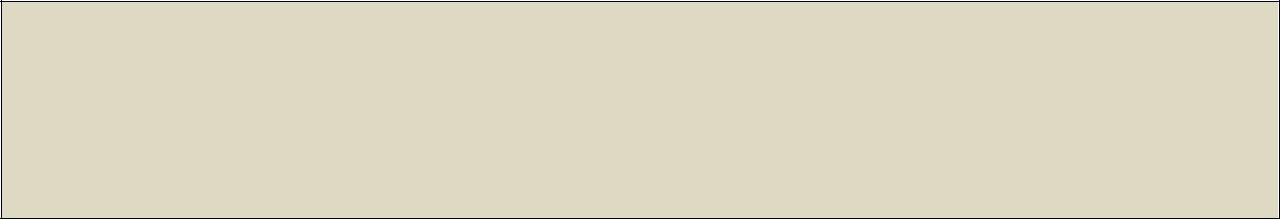
464 | P a g e

**Audit:**

Run the following commands to verify that TMOUT is configured to include a timeout of no more than 900 seconds, to be readonly, and to be exported:

Run the following command to verify that TMOUT is configured in: a .sh file in

/etc/profile.d/:



* for f in /etc/profile.d/\*.sh ; do grep -Eq '(^|^[^#]\*;)\s\*(readonly|export(\s+[^$#;]+\s\*)\*)?\s\*TMOUT=(900|[1-8][0-9][0-9]|[1-9][0-9]|[1-9])\b' $f && grep -Eq '(^|^[^#]\*;)\s\*readonly\s+TMOUT\b' $f && grep -Eq '(^|^[^#]\*;)\s\*export\s+([^$#;]+\s+)\*TMOUT\b' $f && echo "TMOUT correctly configured in file: $f"; done

TMOUT correctly configured in file: <name of file where TMOUT is configured>

Run the following command to verify that TMOUT is not set to a longer timeout:



* grep -PR '^\s\*([^$#;]+\s+)\*TMOUT=(9[0-9][1-9]|0+|[1-9]\d{3,})\b\s\*(\S+\s\*)\*(\s+#.\*)?$' /etc/profile\* /etc/bashrc.bashrc\*

Nothing should be returned

**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 a file ending in .sh in the /etc/profile.d/ directory.

*TMOUT configuration examples:*

* As multiple lines:



TMOUT=900

readonly TMOUT

export TMOUT

* As a single line:



readonly TMOUT=900 ; export TMOUT



465 | P a g e

**CIS Controls:**

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



466 | P a g e

*5.4.5 Ensure default user umask is configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The user file-creation mode mask (umask) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (rwxrwxrwx), and for any newly created file it is 0666 (rw-rw-rw-). The umask modifies the default Linux permissions by restricting (masking) these permissions. The umask is not simply subtracted, but is processed bitwise. Bits set in the umask are cleared in the resulting file mode.

* The user creating the directories or files has the discretion of changing the permissions by:

o Issuing the chmod command

1. Choosing a different default umask
   1. Adding the umask command into a User Shell Configuration File, (

.bash\_profile or .bashrc), in their home directory

* 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-----.

* umask can be set with either octal or Symbolic values:

1. 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.

1. Symbolic Value - Represented by a comma separated list for User u, group g, and world/other o.

*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 .bashrc. etc/bashrc also invokes

/etc/profile.d/\*.sh if *non-login* shell, but redirects output to /dev/null if *non-*



467 | P a g e

*interactive.* **Is only executed for *interactive* shells or if BASH\_ENV is set to**

**/etc/bashrc.**

*User Shell Configuration Files:*

* ~/.bash\_profile - Is executed to configure your shell before the initial command prompt. **Is only read by login shells.**
* ~/.bashrc - Is executed for interactive shells. **only read by a shell that's both interactive and non-login**

**Rationale:**

Setting a secure default value for umask ensures that users make a conscious choice about their file permissions. A permissive umask value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

*Notes:*

* *The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked.*
* *Other methods of setting a default user umask exist.*
* *If other methods are in use in your environment they should be audited and the shell configs should be verified to not override.*



468 | P a g e

**Audit:**

Run the following commands to verify:

•

umask 027 or umask u=rwx,g=rx,o= or more restrictive

* No System Wide umask is set that allows for:

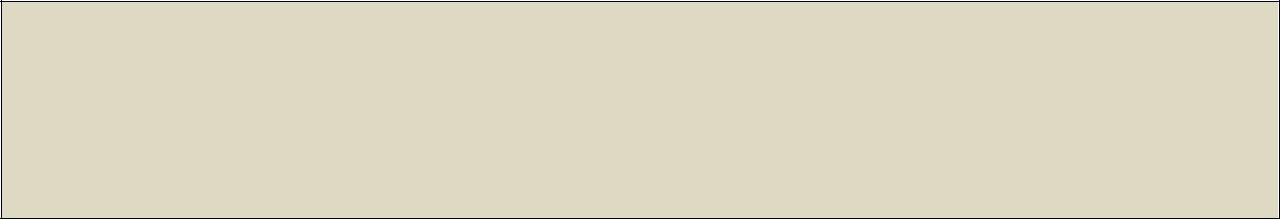
1. A newly created directories's permissions to be less restrictive than 750 (drwxr-x---)
   1. A newly created file's permissions to be less restrictive than 640 (rw-r-----).

* The default System Wide umask is set to enforce:
  1. A newly created directories's permissions to be 750 (drwxr-x---)

1. A newly created file's permissions be 640 (rw-r-----).

Run the following commands to verify if umask is set, it is less restrictive than 027,

u=rwx,g=rx,o=:



* 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/default/login /etc/profile\* /etc/bash.bashrc\*

No file should be returned - May return "No such file or directory"

Run the following command to verify that a System Wide default umask of 027, u=rwx,g=rx,o=, or more restrictive is set:



* grep -REi '^\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/login.defs /etc/default/login /etc/profile\* /etc/bash.bashrc\*

*Example output:*

|  |  |
| --- | --- |
| <full path to file>:UMASK | 027 |
|  |  |



469 | P a g e

**Remediation:**

Configure umask in *one* of the following locations:

•

/etc/login.defs - *Recommended*

* A file ending in .sh in the /etc/profile.d/ directory

•

/etc/default/login

•

/etc/profile.local

•

/etc/profile - *This is not recommended, may be updated/overwritten by YaST2 Online Update*

*Example:*

edit /etc/login.defs and add or modify the UMASK line.



UMASK 027

Review files ending in .sh in the /etc/profile.d/ directory, and the files;

/etc/bash.bashrc, /etc/profile, and /etc/profile.local. Remove or edit all umask

entries to follow local site policy. Any remaining entries should be: umask 027, umask u=rwx,g=rx,o= or more restrictive.

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  |  | |  |
| Maintain documented, standard security configuration standards for all | | | | |  |
|  | authorized operating systems and software. | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Data Protection | | | | |  |  |  |  |
|  |  |  |  |  |



470 | P a g e

*5.5 Ensure root login is restricted to system console (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The file /etc/securetty contains a list of valid terminals that may be logged in directly as root.

**Rationale:**

Since the system console has special properties to handle emergency situations, it is important to ensure that the console is in a physically secure location and that unauthorized consoles have not been defined.

**Audit:**



# cat /etc/securetty

**Remediation:**

Remove entries for any consoles that are not in a physically secure location.

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Establish and maintain a secure configuration process for enterprise assets (end- | | | | | ● | ● | ● |  |
| user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | |  |
|  | and software (operating systems and applications). Review and update documentation | | | | |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this Safeguard. | | | | |  |  |  |  |
|  | 4.6 Securely Manage Enterprise Assets and Software | | | | |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |
|  | Securely manage enterprise assets and software. Example implementations include | | | | |  |  |  |  |
| v8 | managing configuration through version-controlled-infrastructure-as-code and | | | | | ● | ● | ● |  |
| accessing administrative interfaces over secure network protocols, such as Secure Shell | | | | |  |
|  | (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure | | | | |  |  |  |  |
|  | management protocols, such as Telnet (Teletype Network) and HTTP, unless | | | | |  |  |  |  |
|  | operationally essential. | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | ● | ● | ● |  |
|  |  |  | | |  |
| Maintain documented, standard security configuration standards for all authorized | | | | |  |
|  | operating systems and software. | | | | |  |  |  |  |



471 | P a g e

*5.6 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 groups to execute su. This group should be empty to reinforce the use of sudo for privileged access.

**Rationale:**

Restricting the use of su , and using sudo in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via sudo , whereas su can only record that a user executed the su program.

**Audit:**

Run the following command and verify the output matches the line:



# grep -E

'^\s\*auth\s+required\s+pam\_wheel\.so\s+(\S+\s+)\*use\_uid\s+(\S+\s+)\*group=\S+\ s\*(\S+\s\*)\*(\s+#.\*)?$' /etc/pam.d/su

auth required pam\_wheel.so use\_uid group=<group\_name>

Run the following command and verify that the group specified in <group\_name> contains no users:



* grep <group\_name> /etc/group <group\_name>:x:<GID>:

There should be no users listed after the Group ID field.



472 | P a g e

**Remediation:**

Create an empty group that will be specified for use of the su command. The group should be named according to site policy.

*Example*



# groupadd sugroup

Add the following line to the /etc/pam.d/su file, specifying the empty group:



auth required pam\_wheel.so use\_uid group=sugroup

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | ● | ● | ● |  |
|  |  |  | |  |
| Maintain documented, standard security configuration standards for all | | | |  |
|  | authorized operating systems and software. | | | |  |  |  |  |



473 | P a g e

***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.



474 | P a g e

***6.1 System File Permissions***

This section provides guidance on securing aspects of system files and directories.



475 | P a g e

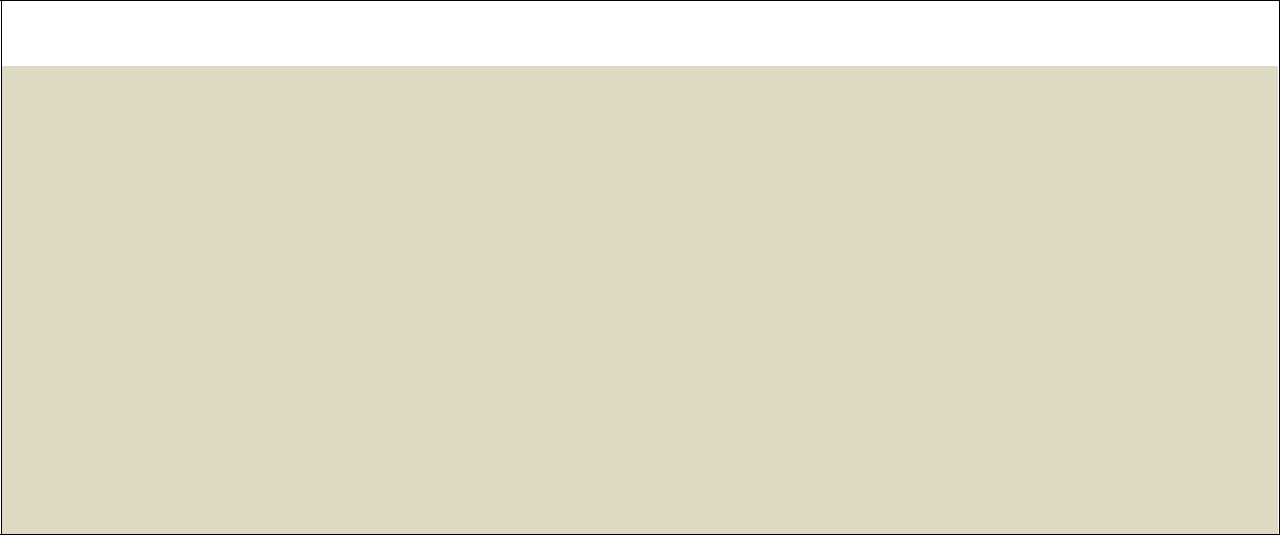
*6.1.1 Audit system file permissions (Manual)*

**Profile Applicability:**

* Level 2 - Server
* Level 2 - Workstation

**Description:**

The RPM package manager has a number of useful options. One of these, the -V option, can be used to verify that system packages are correctly installed. The V option can be used to verify a particular package or to verify all system packages. If no output is returned, the package is installed correctly. The following table describes the meaning of output from the verify option:



|  |  |
| --- | --- |
| Code | Meaning |
|  |  |
| S | File size differs. |

1. File mode differs (includes permissions and file type).

5The MD5 checksum differs.

DThe major and minor version numbers differ on a device file.

LA mismatch occurs in a link.

UThe file ownership differs.

GThe file group owner differs.

TThe file time (mtime) differs.

The rpm -qf command can be used to determine which package a particular file belongs to. For example the following commands determines which package the

/etc/ssh/sshd\_config file belongs to:



# rpm -qf /etc/ssh/sshd\_config

openssh-7.9p1-6.14.1.x86\_64

To verify the settings for the package that controls the /etc/ssh/sshd\_config file, run the following:



* rpm -V openssh-7.9p1-6.14.1.x86\_64

S.5....T. c /etc/ssh/sshd\_config



476 | P a g e

*Note: You can feed the output of the rpm -qf command to the rpm -V command:*



* rpm -V $(rpm -qf /etc/ssh/sshd\_config)

S.5....T. c /etc/ssh/sshd\_config

*Notes:*

* *Since packages and important files may change with new updates and releases, it is recommended to verify everything, not just a finite list of files. This can be a time consuming task and results may depend on site policy therefore it is not a scorable benchmark item, but is provided for those interested in additional security measures.*
* *Some of the recommendations of this benchmark alter the state of files audited by this recommendation. The audit command will alert for all changes to a file permissions even if the new state is more secure than the default.*

**Rationale:**

It is important to confirm that packaged system files and directories are maintained with the permissions they were intended to have from the OS distributor or in accordance with local site policy.

**Audit:**

Run the following command to review all installed packages. Note that this may be very time consuming and may be best scheduled via the cron utility. It is recommended that the output of this command be redirected to a file that can be reviewed later. This command will ignore configuration files due to the extreme likelihood that they will change.



# rpm -Va --nomtime --nosize --nomd5 --nolinkto > <filename> | grep -vw c

**Remediation:**

Investigate the results to ensure any discrepancies found are understood and support proper secure operation of the system.

**References:**

1. <https://docs.fedoraproject.org/en-US/fedora/rawhide/system-administrators-guide/RPM/#s2-rpm-verifying>



477 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



478 | P a g e

*6.1.2 Ensure permissions on /etc/passwd are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/passwd file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

**Rationale:**

It is critical to ensure that the /etc/passwd file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

**Audit:**

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



# stat /etc/passwd

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

**Remediation:**

Run the following commands to set owner, group, and permissions on /etc/passwd:



* chown root:root /etc/passwd
* chmod u-x,g-wx,o-wx /etc/passwd

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



479 | P a g e

*6.1.3 Ensure permissions on /etc/shadow are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/shadow file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

**Rationale:**

If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert the user accounts.

**Audit:**

Run the following command and verify Uid is 0/root, Gid is 0/root or <gid> /shadow, and

Access is 0640 or more restrictive:



# stat /etc/shadow

Access: (0640/-rw-r-----) Uid: ( 0/ root) Gid: ( 15/ shadow)

**Remediation:**

Run the following commands to set owner, group, and permissions on /etc/shadow:



* chown root:root /etc/shadow
* chmod u-x,g-wx,o-rwx /etc/shadow

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



480 | P a g e

*6.1.4 Ensure permissions on /etc/group are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/group file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

**Rationale:**

The /etc/group file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

**Audit:**

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



# stat /etc/group

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

**Remediation:**

Run the following commands to set owner, group, and permissions on /etc/group :



* chown root:root /etc/group
* chmod u-x,g-wx,o-wx /etc/group

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



481 | P a g e

*6.1.5 Ensure permissions on /etc/passwd- are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/passwd- file contains backup user account information.

**Rationale:**

It is critical to ensure that the /etc/passwd- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

**Audit:**

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



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # stat /etc/passwd- |  |  |  |  |  |
| Access: (0644/-rw-r--r--) Uid: ( | 0/ | root) | Gid: ( | 0/ | root) |

**Remediation:**

Run the following commands to set owner, group, and permissions on /etc/passwd- :



* chown root:root /etc/passwd-
* chmod u-x,go-wx /etc/passwd-

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



482 | P a g e

*6.1.6 Ensure permissions on /etc/shadow- are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/shadow- file is used to store backup information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

**Rationale:**

It is critical to ensure that the /etc/shadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

**Audit:**

Run the following command and verify verify Uid is 0/root, Gid is 0/root or /shadow, and

Access is 0640 or more restrictive:



# stat /etc/shadow-

Access: (0640/-rw-r-----) Uid: ( 0/ root) Gid: ( 15/ shadow)

**Remediation:**

Run the following commands to set owner, group, and permissions on /etc/shadow-:



* chown root:shadow /etc/shadow-
* chmod u-x,g-wx,o-rwx /etc/shadow-

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



483 | P a g e

*6.1.7 Ensure permissions on /etc/group- are configured (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The /etc/group- file contains a backup list of all the valid groups defined in the system.

**Rationale:**

It is critical to ensure that the /etc/group- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

**Audit:**

Run the following command and verify Uid and Gid are both 0/root and Access is 0644 or more restrictive:



# stat /etc/group-

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

**Remediation:**

Run the following commands to set owner, group, and permissions on /etc/group-:



* chown root:root /etc/group-
* chmod u-x,go-wx /etc/group-

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



484 | P a g e

*6.1.8 Ensure no world writable files exist (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the chmod(2) man page for more information.

**Rationale:**

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

**Audit:**

Run the following command and verify no files are returned:



* df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -0002

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the --local option to df is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:



# find <partition> -xdev -type f -perm -0002

**Remediation:**

Removing write access for the "other" category ( chmod o-w <filename> ) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.



485 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data access | | | | | | ● | ● | ● |  |
| control lists, also known as access permissions, to local and remote file systems, | | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | | |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | | |  |  |  |  |
|  |  |  |  |  | |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | | |  |  |  |  |
|  | Safeguard. | | | | | |  |  |  |  |
| v7 | 5.1 Establish Secure Configurations | | | | | | ● | ● | ● |  |
|  |  |  |  | | |  |
| Maintain documented, standard security configuration standards for all authorized | | | | | |  |
|  | operating systems and software. | | | | | |  |  |  |  |
| v7 | 13 Data Protection | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| Data Protection | | | | | |  |  |  |  |
|  |  |  |  |  |



486 | P a g e

*6.1.9 Ensure no unowned files or directories exist (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

**Rationale:**

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

**Audit:**

Run the following command and verify no files are returned:



* df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -nouser

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally, the --local option to df is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:



# find <partition> -xdev -nouser

**Remediation:**

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.



487 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.1 Establish and Maintain a Secure Configuration Process | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | | |  |  |  |  |
| v8 |  | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | | ● | ● | ● |  |
|  | and software (operating systems and applications). Review and update documentation | | | | | |  |
|  |  |  |  |  |  |
|  |  | annually, or when significant enterprise changes occur that could impact this | | | | | |  |  |  |  |
|  |  | Safeguard. | | | | | |  |  |  |  |
|  |  | 13.2 Remove Sensitive Data or Systems Not Regularly | | | | | |  |  |  |  |
|  |  |  | |  |  |  | |  |  |  |  |
| v7 |  | Accessed by Organization | | | | | | ● | ● | ● |  |
|  |  | | |  | | |  |
|  | Remove sensitive data or systems not regularly accessed by the organization from | | | | | |  |
|  |  | the network. These systems shall only be used as stand alone systems (disconnected | | | | | |  |  |  |  |
|  |  | from the network) by the business unit needing to occasionally use the system or | | | | | |  |  |  |  |
|  |  | completely virtualized and powered off until needed. | | | | | |  |  |  |  |



488 | P a g e

*6.1.10 Ensure no ungrouped files or directories exist (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups.

**Rationale:**

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

**Audit:**

Run the following command and verify no files are returned:



* df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -nogroup

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the --local option to df is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:



# find <partition> -xdev -nogroup

**Remediation:**

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.



489 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 4.1 Establish and Maintain a Secure Configuration Process | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | | |  |  |  |  |
| v8 |  | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | | ● | ● | ● |  |
|  | and software (operating systems and applications). Review and update documentation | | | | | |  |
|  |  |  |  |  |  |
|  |  | annually, or when significant enterprise changes occur that could impact this | | | | | |  |  |  |  |
|  |  | Safeguard. | | | | | |  |  |  |  |
|  |  | 13.2 Remove Sensitive Data or Systems Not Regularly | | | | | |  |  |  |  |
|  |  |  | |  |  |  | |  |  |  |  |
| v7 |  | Accessed by Organization | | | | | | ● | ● | ● |  |
|  |  | | |  | | |  |
|  | Remove sensitive data or systems not regularly accessed by the organization from | | | | | |  |
|  |  | the network. These systems shall only be used as stand alone systems (disconnected | | | | | |  |  |  |  |
|  |  | from the network) by the business unit needing to occasionally use the system or | | | | | |  |  |  |  |
|  |  | completely virtualized and powered off until needed. | | | | | |  |  |  |  |



490 | P a g e

*6.1.11 Audit SUID executables (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID program is to enable users to perform functions (such as changing their password) that require root privileges.

**Rationale:**

There are valid reasons for SUID programs, but it is important to identify and review such programs to ensure they are legitimate.

**Audit:**

Run the following command to list SUID files:



* df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -4000

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the --local option to df is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:



# find <partition> -xdev -type f -perm -4000

**Remediation:**

Ensure that no rogue SUID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.



491 | P a g e

**CIS Controls:**

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



492 | P a g e

*6.1.12 Audit SGID executables (Manual)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

**Rationale:**

There are valid reasons for SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different md5 checksum than what from the package. This is an indication that the binary may have been replaced.

**Audit:**

Run the following command to list SGID files:



* df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -2000

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the --local option to df is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:



# find <partition> -xdev -type f -perm -2000

**Remediation:**

Ensure that no rogue SGID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.



493 | P a g e

**CIS Controls:**

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



494 | P a g e

***6.2 User and Group Settings***

This section provides guidance on securing aspects of the users and groups.

*Note: The recommendations in this section check local users and groups. Any users or groups from other sources such as LDAP will not be audited. In a domain environment similar checks should be performed against domain users and groups.*



495 | P a g e

*6.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Local accounts can uses shadowed passwords. With shadowed passwords, The passwords are saved in shadow password file, /etc/shadow, encrypted by a salted one-way hash. Accounts with a shadowed password have an x in the second field in /etc/passwd.

**Rationale:**

The /etc/passwd file also contains information like user ID's and group ID's that are used by many system programs. Therefore, the /etc/passwd file must remain world readable. In spite of encoding the password with a randomly-generated one-way hash function, an attacker could still break the system if they got access to the /etc/passwd file. This can be mitigated by using shadowed passwords, thus moving the passwords in the /etc/passwd file to /etc/shadow. The /etc/shadow file is set so only root will be able to read and write. This helps mitigate the risk of an attacker gaining access to the encoded passwords with which to perform a dictionary attack.

*Notes:*

* *All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.*
* *A user account with an empty second field in /etc/passwd allows the account to be logged into by providing only the username.*

**Audit:**

Run the following command and verify that no output is returned:



* awk -F: '($2 != "x" ) { print $1 " is not set to shadowed passwords "}' /etc/passwd



496 | P a g e

**Remediation:**

If any accounts in the /etc/passwd file do not have a single x in the password field, run the following command to set these accounts to use shadowed passwords:



# sed -e 's/^\([a-zA-Z0-9\_]\*\):[^:]\*:/\1:x:/' -i /etc/passwd

Investigate to determine if the account is logged in and what it is being used for, to determine if it needs to be forced off.

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  |  | **Control** | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.11 Encrypt Sensitive Data at Rest | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Encrypt sensitive data at rest on servers, applications, and databases containing | | | | |  |  |  |  |
| v8 | 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 | 4.4 Use Unique Passwords | | | | |  | ● | ● |  |
|  |  | |  | |  |  |
| Where multi-factor authentication is not supported (such as local administrator, | | | | |  |  |
|  | root, or service accounts), accounts will use passwords that are unique to that system. | | | | |  |  |  |  |



497 | P a g e

*6.2.2 Ensure /etc/shadow password fields are not empty (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

An account with an empty password field means that anybody may log in as that user without providing a password.

**Rationale:**

All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.

**Audit:**

Run the following command and verify that no output is returned:



# awk -F: '($2 == "" ) { print $1 " does not have a password "}' /etc/shadow

**Remediation:**

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it can be determined why it does not have a password:



# passwd -l <username>

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be forced off.

**CIS Controls:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |
|  | 5.2 Use Unique Passwords | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| v8 | Use unique passwords for all enterprise assets. Best practice implementation | | | ● | ● | ● |  |
| includes, at a minimum, an 8-character password for accounts using MFA and a 14- | | |  |
|  |  |  |  |  |
|  | character password for accounts not using MFA. | | |  |  |  |  |
| v7 | 4.4 Use Unique Passwords | | |  | ● | ● |  |
|  |  |  |  |  |
| Where multi-factor authentication is not supported (such as local administrator, | | |  |  |
|  | root, or service accounts), accounts will use passwords that are unique to that system. | | |  |  |  |  |



498 | P a g e

*6.2.3 Ensure root is the only UID 0 account (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Any account with UID 0 has superuser privileges on the system.

**Rationale:**

This access must be limited to only the default root account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 5.6 Ensure access to the su command is restricted.

**Audit:**

Run the following command and verify that only "root" is returned:



* awk -F: '($3 == 0) { print $1 }' /etc/passwd root

**Remediation:**

Remove any users other than root with UID 0 or assign them a new UID if appropriate.

**CIS Controls:**

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



499 | P a g e

*6.2.4 Ensure root PATH Integrity (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

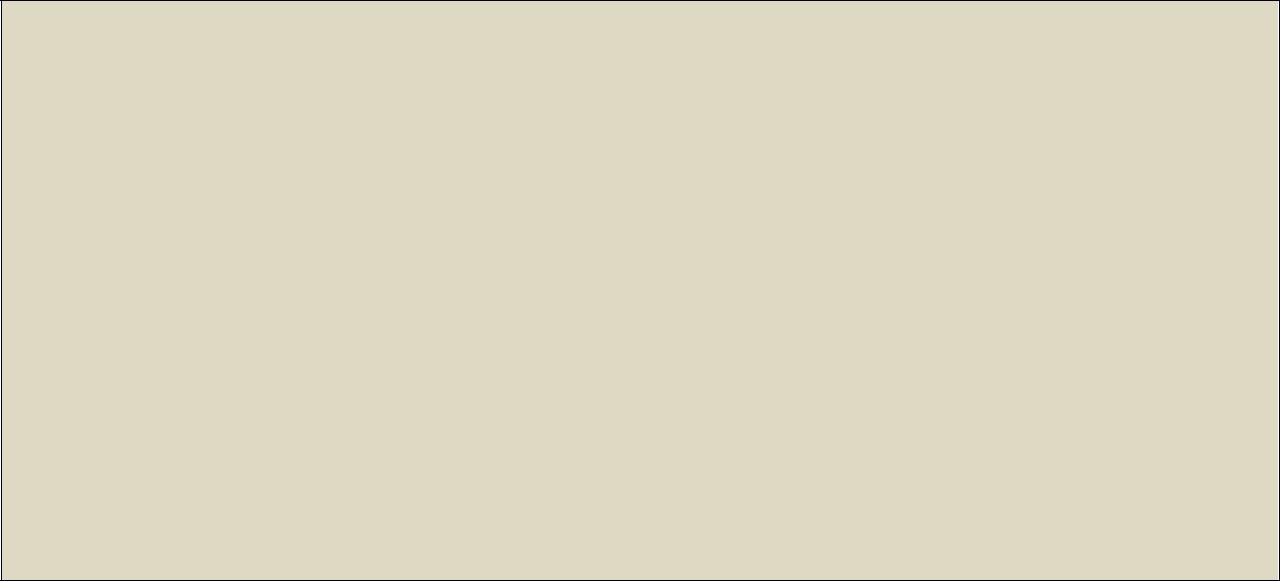
The root user can execute any command on the system and could be fooled into executing programs unintentionally if the PATH is not set correctly.

**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

if echo "$PATH" | grep -q "::" ; then

echo "Empty Directory in PATH (::)"

fi

if echo "$PATH" | grep -q ":$" ; then

echo "Trailing : in PATH"

fi

for x in $(echo "$PATH" | 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.



500 | P a g e

**CIS Controls:**

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



501 | P a g e

*6.2.5 Ensure all users' home directories exist (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Users can be defined in /etc/passwd without a home directory or with a home directory that does not actually exist.

**Rationale:**

If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

**Audit:**

Run the following script and verify no results are returned:



#!/bin/bash

grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read -r user dir; do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist."

fi

done

*Note: The audit script checks all users with interactive shells except halt, sync, shutdown, and nfsnobody.*

**Remediation:**

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.



502 | P a g e

**CIS Controls:**

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



503 | P a g e

*6.2.6 Ensure users' home directories permissions are 750 or more restrictive (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

**Rationale:**

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

**Audit:**

Run the following script and verify no results are returned:



#!/bin/bash

grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist." else

dirperm=$(ls -ld $dir | cut -f1 -d" ")

if [ $(echo $dirperm | cut -c6) != "-" ]; then

echo "Group Write permission set on the home directory ($dir) of user

$user"

fi

if [ $(echo $dirperm | cut -c8) != "-" ]; then

echo "Other Read permission set on the home directory ($dir) of user

$user"

fi

if [ $(echo $dirperm | cut -c9) != "-" ]; then

echo "Other Write permission set on the home directory ($dir) of user

$user"

fi

if [ $(echo $dirperm | cut -c10) != "-" ]; then

echo "Other Execute permission set on the home directory ($dir) of user

$user"

fi

fi

done



504 | P a g e

**Remediation:**

Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



505 | P a g e

*6.2.7 Ensure users own their home directories (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

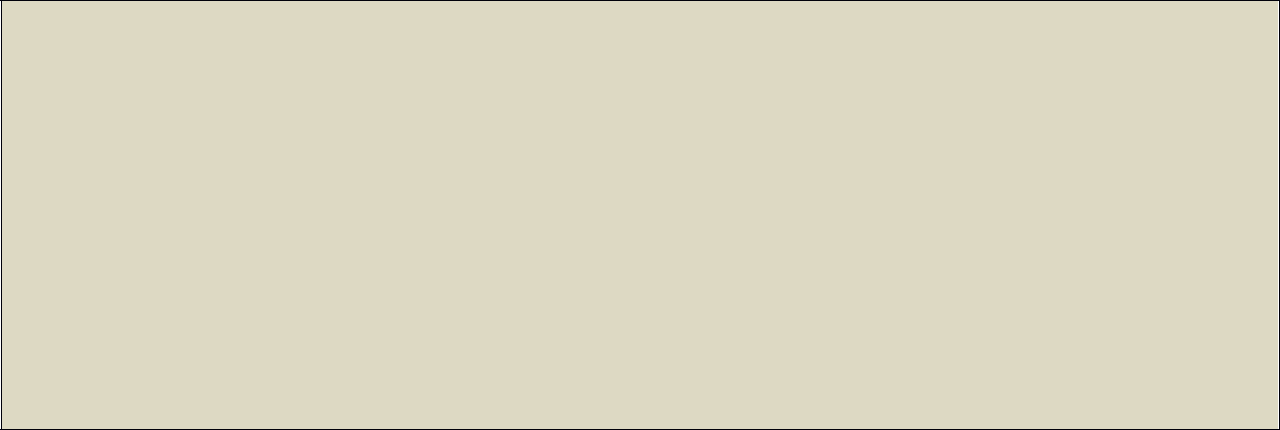
The user home directory is space defined for the particular user to set local environment variables and to store personal files.

**Rationale:**

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

**Audit:**

Run the following script and verify no results are returned:



#!/bin/bash

grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist." else

owner=$(stat -L -c "%U" "$dir")

if [ "$owner" != "$user" ]; then

echo "The home directory ($dir) of user $user is owned by $owner."

fi

fi

done

**Remediation:**

Change the ownership of any home directories that are not owned by the defined user to the correct user.



506 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



507 | P a g e

*6.2.8 Ensure users' dot files are not group or world writable (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

**Rationale:**

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

**Audit:**

Run the following script and verify no results are returned:



#!/bin/bash

grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist." else

for file in $dir/.[A-Za-z0-9]\*; do

if [ ! -h "$file" -a -f "$file" ]; then fileperm=$(ls -ld $file | cut -f1 -d" ")

if [ $(echo $fileperm | cut -c6) != "-" ]; then echo "Group Write permission set on file $file"

fi

if [ $(echo $fileperm | cut -c9) != "-" ]; then echo "Other Write permission set on file $file"

fi

fi

done

fi

done

**Remediation:**

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.



508 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



509 | P a g e

*6.2.9 Ensure no users have .forward files (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

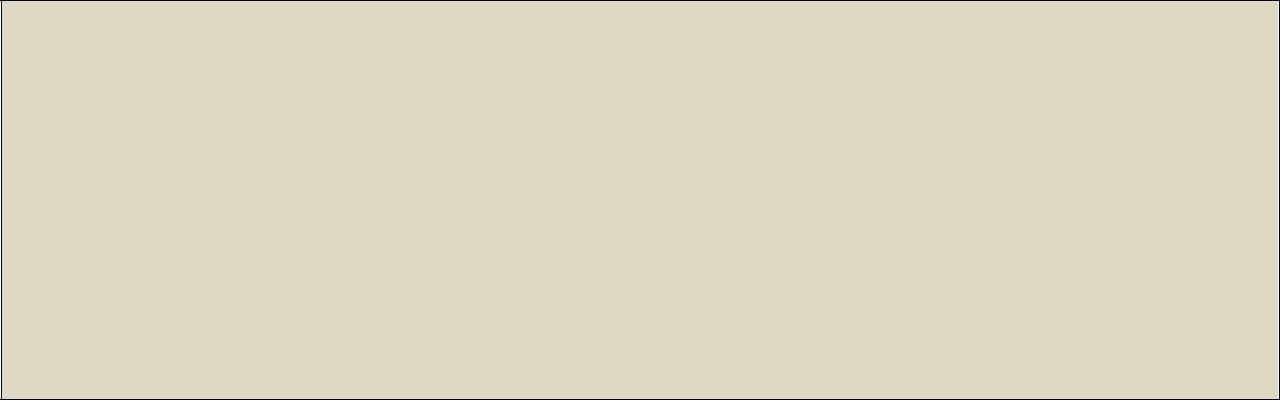
The .forward file specifies an email address to forward the user's mail to.

**Rationale:**

Use of the .forward file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The .forward file also poses a risk as it can be used to execute commands that may perform unintended actions.

**Audit:**

Run the following script and verify no results are returned:



#!/bin/bash

awk -F: '($1 !~ /^(root|halt|sync|shutdown)$/ && $7 != "'"$(which nologin)"'"

* $7 != "/bin/false" && $7 != "/usr/bin/false") { print $1 " " $6 }' /etc/passwd | while read user dir; do

if [ ! -d "$dir" ] ; then

echo "The home directory ($dir) of user $user does not exist." else

if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ] ; then echo ".forward file $dir/.forward exists"

fi

fi done

**Remediation:**

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .forward files and determine the action to be taken in accordance with site policy.



510 | P a g e

**CIS Controls:**

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



511 | P a g e

*6.2.10 Ensure no users have .netrc files (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

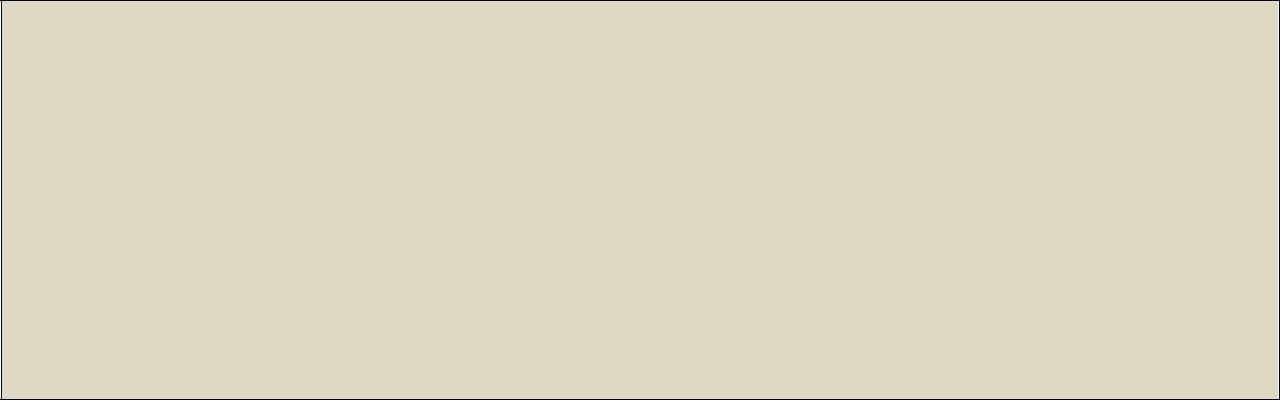
The .netrc file contains data for logging into a remote host for file transfers via FTP.

**Rationale:**

The .netrc file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over .netrc files from other systems which could pose a risk to those systems.

**Audit:**

Run the following script and verify no results are returned:



#!/bin/bash

awk -F: '($1 !~ /^(root|halt|sync|shutdown)$/ && $7 != "'"$(which nologin)"'"

* $7 != "/bin/false" && $7 != "/usr/bin/false") { print $1 " " $6 }' /etc/passwd | while read user dir; do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist." else

if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then echo ".netrc file $dir/.netrc exists"

fi

fi done

**Remediation:**

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.



512 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.6 Securely Manage Enterprise Assets and Software | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Securely manage enterprise assets and software. Example implementations include | | | | |  |  |  |  |
| v8 | managing configuration through version-controlled-infrastructure-as-code and | | | | | ● | ● | ● |  |
| accessing administrative interfaces over secure network protocols, such as Secure Shell | | | | |  |
|  | (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure | | | | |  |  |  |  |
|  | management protocols, such as Telnet (Teletype Network) and HTTP, unless | | | | |  |  |  |  |
|  | operationally essential. | | | | |  |  |  |  |
| v7 | 16.4 Encrypt or Hash all Authentication Credentials | | | | |  | ● | ● |  |
|  |  |  |  |  |  |  |
| Encrypt or hash with a salt all authentication credentials when stored. | | | | |  |  |
|  |  |  |  |  |



513 | P a g e

*6.2.11 Ensure users' .netrc Files are not group or world accessible (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

While the system administrator can establish secure permissions for users' .netrc files, the users can easily override these.

**Rationale:**

.netrc files may contain unencrypted passwords that may be used to attack other systems.

*Note: While the complete removal of .netrc files is recommended if any are required on the system secure permissions must be applied.*



514 | P a g e

**Audit:**

Run the following script and verify no results are returned:



#!/bin/bash

awk -F: '($1 !~ /^(root|halt|sync|shutdown)$/ && $7 != "'"$(which nologin)"'"

* $7 != "/bin/false" && $7 != "/usr/bin/false") { print $1 " " $6 }' /etc/passwd | while read user dir; do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist." else

for file in $dir/.netrc; do

if [ ! -h "$file" -a -f "$file" ]; then fileperm=$(ls -ld $file | cut -f1 -d" ")

if [ $(echo $fileperm | cut -c5) != "-" ]; then echo "Group Read set on $file"

fi

if [ $(echo $fileperm | cut -c6) != "-" ]; then echo "Group Write set on $file"

fi

if [ $(echo $fileperm | cut -c7) != "-" ]; then echo "Group Execute set on $file"

fi

if [ $(echo $fileperm | cut -c8) != "-" ]; then echo "Other Read set on $file"

fi

if [ $(echo $fileperm | cut -c9) != "-" ]; then echo "Other Write set on $file"

fi

if [ $(echo $fileperm | cut -c10) != "-" ]; then echo "Other Execute set on $file"

fi

fi done

fi done

**Remediation:**

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .netrc file permissions and determine the action to be taken in accordance with site policy.



515 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file systems, | | | | |  |
|  |  |  |  |  |
|  | databases, and applications. | | | | |  |  |  |  |
|  | 14.6 Protect Information through Access Control Lists | | | | |  |  |  |  |
|  |  | |  | |  |  |  |  |  |
| v7 | Protect all information stored on systems with file system, network share, claims, | | | | | ● | ● | ● |  |
| application, or database specific access control lists. These controls will enforce the | | | | |  |
|  | principle that only authorized individuals should have access to the information based | | | | |  |  |  |  |
|  | on their need to access the information as a part of their responsibilities. | | | | |  |  |  |  |



516 | P a g e

*6.2.12 Ensure no users have .rhosts files (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

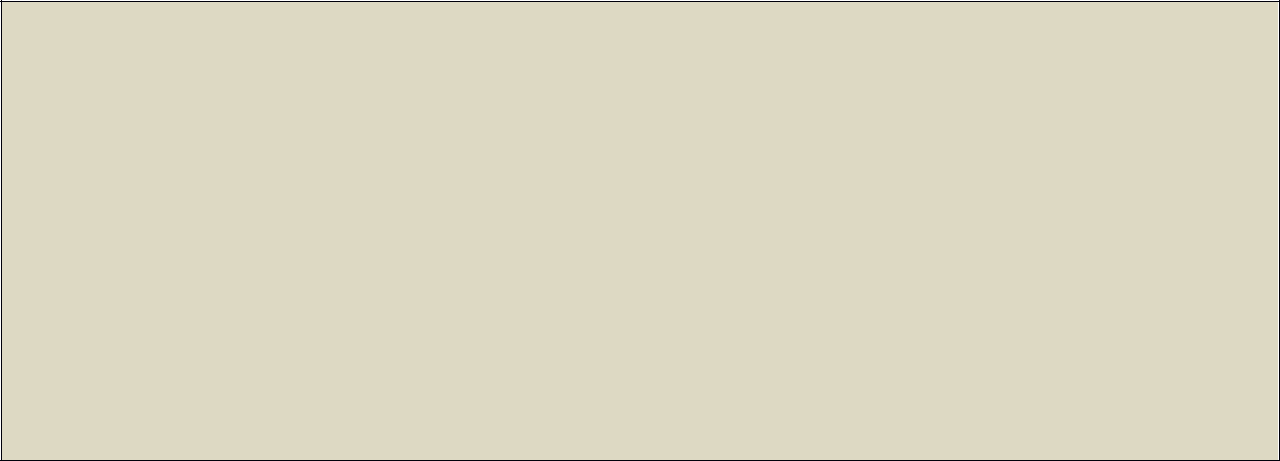
While no .rhosts files are shipped by default, users can easily create them.

**Rationale:**

This action is only meaningful if .rhosts support is permitted in the file /etc/pam.conf . Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf , they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

**Audit:**

Run the following script and verify no results are returned:



#!/bin/bash

awk -F: '($1 !~ /^(root|halt|sync|shutdown)$/ && $7 != "'"$(which nologin)"'"

* $7 != "/bin/false" && $7 != "/usr/bin/false") { print $1 " " $6 }' /etc/passwd | while read user dir; do

if [ ! -d "$dir" ]; then

echo "The home directory ($dir) of user $user does not exist." else

for file in $dir/.rhosts; do

if [ ! -h "$file" -a -e "$file" ]; then echo ".rhosts file in $dir"

fi done

fi done

**Remediation:**

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .rhosts files and determine the action to be taken in accordance with site policy.



517 | P a g e

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | | |  |  |  |  |
|  | Safeguard. | | | | |  |  |  |  |
| v7 | 16.4 Encrypt or Hash all Authentication Credentials | | | | |  | ● | ● |  |
|  |  |  |  |  |  |  |
| Encrypt or hash with a salt all authentication credentials when stored. | | | | |  |  |
|  |  |  |  |  |



518 | P a g e

*6.2.13 Ensure all groups in /etc/passwd exist in /etc/group (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

Over time, system administration errors and changes can lead to groups being defined in

/etc/passwd but not in /etc/group .

**Rationale:**

Groups defined in the /etc/passwd file but not in the /etc/group file pose a threat to system security since group permissions are not properly managed.

**Audit:**

Run the following script and verify no results are returned:



#!/bin/bash

for i in $(cut -s -d: -f4 /etc/passwd | sort -u ); do

grep -q -P "^.\*?:[^:]\*:$i:" /etc/group

if [ $? -ne 0 ]; then

echo "Group $i is referenced by /etc/passwd but does not exist in /etc/group"

fi

done

**Remediation:**

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 3.3 Configure Data Access Control Lists | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| v8 | Configure data access control lists based on a user’s need to know. Apply data | | | | ● | ● | ● |  |
| access control lists, also known as access permissions, to local and remote file | | | |  |
|  |  |  |  |  |
|  | systems, databases, and applications. | | | |  |  |  |  |
| v7 | 16 Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |



519 | P a g e

*6.2.14 Ensure no duplicate UIDs exist (Automated)*

**Profile Applicability:**

* Level 1 - Server
* Level 1 - Workstation

**Description:**

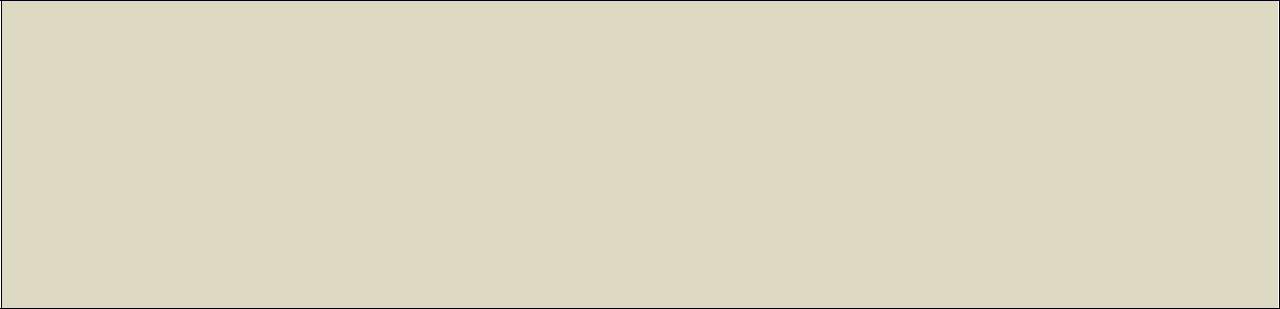
Although the useradd program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the /etc/passwd file and change the UID field.

**Rationale:**

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

**Audit:**

Run the following script and verify no results are returned:



#!/bin/bash

cut -f3 -d":" /etc/passwd | sort -n | uniq -c | while read x ; do [ -z "$x" ] && break

set - $x

if [ $1 -gt 1 ]; then

users=$(awk -F: '($3 == n) { print $1 }' n=$2 /etc/passwd | xargs)

echo "Duplicate UID ($2): $users"

fi

done

**Remediation:**

Based on the results of the audit script, establish unique UIDs and review all files owned by the shared UIDs to determine which UID they are supposed to belong to.

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | |  |  |  |  |
|  | Safeguard. | | | |  |  |  |  |
| v7 | 16 Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |



520 | P a g e

*6.2.15 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.

*Note: You can also use the grpck command to check for other inconsistencies in the*

*/etc/group file.*

**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.

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | |  |  |  |  |
|  | Safeguard. | | | |  |  |  |  |
| v7 | 16 Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |



521 | P a g e

*6.2.16 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 .

*Example: If "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem*

**Audit:**

Run the following script and verify no results are returned:



#!/bin/bash

cut -d: -f1 /etc/passwd | sort | uniq -d | while read x do echo "Duplicate login name ${x} in /etc/passwd" done

**Remediation:**

Based on the results of the audit script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | |  |  |  |  |
|  | Safeguard. | | | |  |  |  |  |
| v7 | 16 Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |



522 | P a g e

*6.2.17 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 x do echo "Duplicate group name ${x} in /etc/group" done

**Remediation:**

Based on the results of the audit script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

**CIS Controls:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Controls** |  | **Control** | | | **IG 1** | **IG 2** | **IG 3** |  |
| **Version** |  |  |
|  |  |  |  |  |  |  |  |
|  | 4.1 Establish and Maintain a Secure Configuration Process | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | Establish and maintain a secure configuration process for enterprise assets (end- | | | |  |  |  |  |
| v8 | user devices, including portable and mobile, non-computing/IoT devices, and servers) | | | | ● | ● | ● |  |
| and software (operating systems and applications). Review and update documentation | | | |  |
|  |  |  |  |  |
|  | annually, or when significant enterprise changes occur that could impact this | | | |  |  |  |  |
|  | Safeguard. | | | |  |  |  |  |
| v7 | 16 Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Account Monitoring and Control | | | |  |  |  |  |
|  |  |  |  |  |



523 | P a g e

*6.2.18 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:



* grep ^shadow:[^:]\*:[^:]\*:[^:]+ /etc/group
* awk -F: '($4 == "<shadow-gid>") { print }' /etc/passwd

**Remediation:**

Remove all users from the shadow group, and change the primary group of any users with shadow as their primary group.

**CIS Controls:**

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



524 | P a g e

**Appendix: Recommendation Summary Table**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Control** |  | **Set** | |  |
|  |  |  |  | **Correctly** | |  |
|  |  |  |  | Yes | No |  |
|  | **1** | **Initial Setup** |  |  |  |  |
|  | **1.1** | **Filesystem Configuration** |  |  |  |  |
|  | **1.1.1** | **Disable unused filesystems** |  |  |  |  |
|  | 1.1.1.1 | Ensure mounting of squashfs filesystems is disabled |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 1.1.1.2 | Ensure mounting of udf filesystems is disabled (Automated) |  |  |  |  |
|  | 1.1.1.3 | Ensure mounting of FAT filesystems is limited (Automated) |  |  |  |  |
|  | 1.1.2 | Ensure /tmp is configured (Automated) |  |  |  |  |
|  | 1.1.3 | Ensure noexec option set on /tmp partition (Automated) |  |  |  |  |
|  | 1.1.4 | Ensure nodev option set on /tmp partition (Automated) |  |  |  |  |
|  | 1.1.5 | Ensure nosuid option set on /tmp partition (Automated) |  |  |  |  |
|  | 1.1.6 | Ensure /dev/shm is configured (Automated) |  |  |  |  |
|  | 1.1.7 | Ensure noexec option set on /dev/shm partition |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 1.1.8 | Ensure nodev option set on /dev/shm partition |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 1.1.9 | Ensure nosuid option set on /dev/shm partition |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 1.1.10 | Ensure separate partition exists for /var (Automated) |  |  |  |  |
|  | 1.1.11 | Ensure separate partition exists for /var/tmp (Automated) |  |  |  |  |
|  | 1.1.12 | Ensure noexec option set on /var/tmp partition |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 1.1.13 | Ensure nodev option set on /var/tmp partition (Automated) |  |  |  |  |
|  | 1.1.14 | Ensure nosuid option set on /var/tmp partition |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 1.1.15 | Ensure separate partition exists for /var/log (Automated) |  |  |  |  |
|  | 1.1.16 | Ensure separate partition exists for /var/log/audit |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 1.1.17 | Ensure separate partition exists for /home (Automated) |  |  |  |  |
|  | 1.1.18 | Ensure nodev option set on /home partition (Automated) |  |  |  |  |
|  | 1.1.19 | Ensure noexec option set on removable media partitions |  |  |  |  |
|  |  | (Manual) |  |  |  |  |
|  | 1.1.20 | Ensure nodev option set on removable media partitions |  |  |  |  |
|  |  | (Manual) |  |  |  |  |
|  | 1.1.21 | Ensure nosuid option set on removable media partitions |  |  |  |  |
|  |  | (Manual) |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  | 525 | P a g e | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1.1.22 | Ensure sticky bit is set on all world-writable directories |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 1.1.23 | Disable Automounting (Automated) |  |  |  |  |
|  | **1.2** | **Configure Software Updates** |  |  |  |  |
|  | 1.2.1 | Ensure GPG keys are configured (Manual) |  |  |  |  |
|  | 1.2.2 | Ensure package manager repositories are configured |  |  |  |  |
|  |  | (Manual) |  |  |  |  |
|  | 1.2.3 | Ensure gpgcheck is globally activated (Automated) |  |  |  |  |
|  | **1.3** | **Configure sudo** |  |  |  |  |
|  | 1.3.1 | Ensure sudo is installed (Automated) |  |  |  |  |
|  | 1.3.2 | Ensure sudo commands use pty (Automated) |  |  |  |  |
|  | 1.3.3 | Ensure sudo log file exists (Automated) |  |  |  |  |
|  | **1.4** | **Filesystem Integrity Checking** |  |  |  |  |
|  | 1.4.1 | Ensure AIDE is installed (Automated) |  |  |  |  |
|  | 1.4.2 | Ensure filesystem integrity is regularly checked |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | **1.5** | **Secure Boot Settings** |  |  |  |  |
|  | 1.5.1 | Ensure bootloader password is set (Automated) |  |  |  |  |
|  | 1.5.2 | Ensure permissions on bootloader config are configured |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 1.5.3 | Ensure authentication required for single user mode |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | **1.6** | **Additional Process Hardening** |  |  |  |  |
|  | 1.6.1 | Ensure core dumps are restricted (Automated) |  |  |  |  |
|  | 1.6.2 | Ensure XD/NX support is enabled (Automated) |  |  |  |  |
|  | 1.6.3 | Ensure address space layout randomization (ASLR) is |  |  |  |  |
|  |  | enabled (Automated) |  |  |  |  |
|  | 1.6.4 | Ensure prelink is disabled (Automated) |  |  |  |  |
|  | **1.7** | **Mandatory Access Control** |  |  |  |  |
|  | **1.7.1** | **Configure AppArmor** |  |  |  |  |
|  | 1.7.1.1 | Ensure AppArmor is installed (Automated) |  |  |  |  |
|  | 1.7.1.2 | Ensure AppArmor is enabled in the bootloader |  |  |  |  |
|  |  | configuration (Automated) |  |  |  |  |
|  | 1.7.1.3 | Ensure all AppArmor Profiles are in enforce or complain |  |  |  |  |
|  |  | mode (Automated) |  |  |  |  |
|  | 1.7.1.4 | Ensure all AppArmor Profiles are enforcing (Automated) |  |  |  |  |
|  | **1.8** | **Warning Banners** |  |  |  |  |
|  | **1.8.1** | **Command Line Warning Banners** |  |  |  |  |
|  | 1.8.1.1 | Ensure message of the day is configured properly |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 1.8.1.2 | Ensure local login warning banner is configured properly |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 1.8.1.3 | Ensure remote login warning banner is configured properly |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  | 526 | P a g e | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1.8.1.4 | Ensure permissions on /etc/motd are configured |  |  |
|  | (Automated) |  |  |
| 1.8.1.5 | Ensure permissions on /etc/issue are configured |  |  |
|  | (Automated) |  |  |
| 1.8.1.6 | Ensure permissions on /etc/issue.net are configured |  |  |
|  | (Automated) |  |  |
| 1.9 | Ensure updates, patches, and additional security software |  |  |
|  | are installed (Manual) |  |  |
| 1.10 | Ensure GDM is removed or login is configured (Automated) |  |  |
| **2** | **Services** |  |  |
| **2.1** | **inetd Services** |  |  |
| 2.1.1 | Ensure xinetd is not installed (Automated) |  |  |
| **2.2** | **Special Purpose Services** |  |  |
| **2.2.1** | **Time Synchronization** |  |  |
| 2.2.1.1 | Ensure time synchronization is in use (Automated) |  |  |
| 2.2.1.2 | Ensure systemd-timesyncd is configured (Manual) |  |  |
| 2.2.1.3 | Ensure chrony is configured (Automated) |  |  |
| 2.2.2 | Ensure X11 Server components are not installed |  |  |
|  | (Automated) |  |  |
| 2.2.3 | Ensure Avahi Server is not installed (Automated) |  |  |
| 2.2.4 | Ensure CUPS is not installed (Automated) |  |  |
| 2.2.5 | Ensure DHCP Server is not installed (Automated) |  |  |
| 2.2.6 | Ensure LDAP server is not installed (Automated) |  |  |
| 2.2.7 | Ensure nfs-utils is not installed or the nfs-server service is |  |  |
|  | masked (Automated) |  |  |
| 2.2.8 | Ensure rpcbind is not installed or the rpcbind services are |  |  |
|  | masked (Automated) |  |  |
| 2.2.9 | Ensure DNS Server is not installed (Automated) |  |  |
| 2.2.10 | Ensure FTP Server is not installed (Automated) |  |  |
| 2.2.11 | Ensure HTTP server is not installed (Automated) |  |  |
| 2.2.12 | Ensure IMAP and POP3 server is not installed (Automated) |  |  |
| 2.2.13 | Ensure Samba is not installed (Automated) |  |  |
| 2.2.14 | Ensure HTTP Proxy Server is not installed (Automated) |  |  |
| 2.2.15 | Ensure net-snmp is not installed (Automated) |  |  |
| 2.2.16 | Ensure mail transfer agent is configured for local-only mode |  |  |
|  | (Automated) |  |  |
| 2.2.17 | Ensure rsync is not installed or the rsyncd service is masked |  |  |
|  | (Automated) |  |  |
| 2.2.18 | Ensure NIS server is not installed (Automated) |  |  |
| 2.2.19 | Ensure telnet-server is not installed (Automated) |  |  |
| **2.3** | **Service Clients** |  |  |
| 2.3.1 | Ensure NIS Client is not installed (Automated) |  |  |
| 2.3.2 | Ensure rsh client is not installed (Automated) |  |  |
| 2.3.3 | Ensure talk client is not installed (Automated) |  |  |



527 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 2.3.4 | Ensure telnet client is not installed (Automated) |  |  |
| 2.3.5 | Ensure LDAP client is not installed (Automated) |  |  |
| 2.4 | Ensure nonessential services are removed or masked |  |  |
|  | (Manual) |  |  |
| **3** | **Network Configuration** |  |  |
| **3.1** | **Disable unused network protocols and devices** |  |  |
| 3.1.1 | Disable IPv6 (Automated) |  |  |
| 3.1.2 | Ensure wireless interfaces are disabled (Manual) |  |  |
| **3.2** | **Network Parameters (Host Only)** |  |  |
| 3.2.1 | Ensure IP forwarding is disabled (Automated) |  |  |
| 3.2.2 | Ensure packet redirect sending is disabled (Automated) |  |  |
| **3.3** | **Network Parameters (Host and Router)** |  |  |
| 3.3.1 | Ensure source routed packets are not accepted (Automated) |  |  |
| 3.3.2 | Ensure ICMP redirects are not accepted (Automated) |  |  |
| 3.3.3 | Ensure secure ICMP redirects are not accepted (Automated) |  |  |
| 3.3.4 | Ensure suspicious packets are logged (Automated) |  |  |
| 3.3.5 | Ensure broadcast ICMP requests are ignored (Automated) |  |  |
| 3.3.6 | Ensure bogus ICMP responses are ignored (Automated) |  |  |
| 3.3.7 | Ensure Reverse Path Filtering is enabled (Automated) |  |  |
| 3.3.8 | Ensure TCP SYN Cookies is enabled (Automated) |  |  |
| 3.3.9 | Ensure IPv6 router advertisements are not accepted |  |  |
|  | (Automated) |  |  |
| **3.4** | **Uncommon Network Protocols** |  |  |
| 3.4.1 | Ensure DCCP is disabled (Automated) |  |  |
| 3.4.2 | Ensure SCTP is disabled (Automated) |  |  |
| **3.5** | **Firewall Configuration** |  |  |
| **3.5.1** | **Configure firewalld** |  |  |
| 3.5.1.1 | Ensure FirewallD is installed (Automated) |  |  |
| 3.5.1.2 | Ensure nftables is not installed or stopped and masked |  |  |
|  | (Automated) |  |  |
| 3.5.1.3 | Ensure firewalld service is enabled and running |  |  |
|  | (Automated) |  |  |
| 3.5.1.4 | Ensure default zone is set (Automated) |  |  |
| 3.5.1.5 | Ensure network interfaces are assigned to appropriate zone |  |  |
|  | (Manual) |  |  |
| 3.5.1.6 | Ensure unnecessary services and ports are not accepted |  |  |
|  | (Manual) |  |  |
| **3.5.2** | **Configure nftables** |  |  |
| 3.5.2.1 | Ensure nftables is installed (Automated) |  |  |
| 3.5.2.2 | Ensure firewalld is not installed or stopped and masked |  |  |
|  | (Automated) |  |  |
| 3.5.2.3 | Ensure iptables are flushed (Manual) |  |  |
| 3.5.2.4 | Ensure a table exists (Automated) |  |  |
| 3.5.2.5 | Ensure base chains exist (Automated) |  |  |



528 | P a g e

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 3.5.2.6 | Ensure loopback traffic is configured (Automated) |  |  |  |  |
|  | 3.5.2.7 | Ensure outbound and established connections are |  |  |  |  |
|  |  | configured (Manual) |  |  |  |  |
|  | 3.5.2.8 | Ensure default deny firewall policy (Automated) |  |  |  |  |
|  | 3.5.2.9 | Ensure nftables service is enabled (Automated) |  |  |  |  |
|  | 3.5.2.10 | Ensure nftables rules are permanent (Automated) |  |  |  |  |
|  | **3.5.3** | **Configure iptables** |  |  |  |  |
|  | **3.5.3.1** | **Configure software** |  |  |  |  |
|  | 3.5.3.1.1 | Ensure iptables package is installed (Automated) |  |  |  |  |
|  | 3.5.3.1.2 | Ensure nftables is not installed (Automated) |  |  |  |  |
|  | 3.5.3.1.3 | Ensure firewalld is not installed or stopped and masked |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | **3.5.3.2** | **Configure IPv4 iptables** |  |  |  |  |
|  | 3.5.3.2.1 | Ensure default deny firewall policy (Automated) |  |  |  |  |
|  | 3.5.3.2.2 | Ensure loopback traffic is configured (Automated) |  |  |  |  |
|  | 3.5.3.2.3 | Ensure outbound and established connections are |  |  |  |  |
|  |  | configured (Manual) |  |  |  |  |
|  | 3.5.3.2.4 | Ensure firewall rules exist for all open ports (Automated) |  |  |  |  |
|  | **3.5.3.3** | **Configure IPv6 ip6tables** |  |  |  |  |
|  | 3.5.3.3.1 | Ensure IPv6 default deny firewall policy (Automated) |  |  |  |  |
|  | 3.5.3.3.2 | Ensure IPv6 loopback traffic is configured (Automated) |  |  |  |  |
|  | 3.5.3.3.3 | Ensure IPv6 outbound and established connections are |  |  |  |  |
|  |  | configured (Manual) |  |  |  |  |
|  | 3.5.3.3.4 | Ensure IPv6 firewall rules exist for all open ports (Manual) |  |  |  |  |
|  | **4** | **Logging and Auditing** |  |  |  |  |
|  | **4.1** | **Configure System Accounting (auditd)** |  |  |  |  |
|  | **4.1.1** | **Ensure auditing is enabled** |  |  |  |  |
|  | 4.1.1.1 | Ensure auditd is installed (Automated) |  |  |  |  |
|  | 4.1.1.2 | Ensure auditd service is enabled and running (Automated) |  |  |  |  |
|  | 4.1.1.3 | Ensure auditing for processes that start prior to auditd is |  |  |  |  |
|  |  | enabled (Automated) |  |  |  |  |
|  | **4.1.2** | **Configure Data Retention** |  |  |  |  |
|  | 4.1.2.1 | Ensure audit log storage size is configured (Automated) |  |  |  |  |
|  | 4.1.2.2 | Ensure audit logs are not automatically deleted |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 4.1.2.3 | Ensure system is disabled when audit logs are full |  |  |  |  |
|  |  | (Automated) |  |  |  |  |
|  | 4.1.2.4 | Ensure audit\_backlog\_limit is sufficient (Automated) |  |  |  |  |
|  | 4.1.3 | Ensure events that modify date and time information are |  |  |  |  |
|  |  | collected (Automated) |  |  |  |  |
|  | 4.1.4 | Ensure events that modify user/group information are |  |  |  |  |
|  |  | collected (Automated) |  |  |  |  |
|  | 4.1.5 | Ensure events that modify the system's network |  |  |  |  |
|  |  | environment are collected (Automated) |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  | 529 | P a g e | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 4.1.6 | Ensure events that modify the system's Mandatory Access |  |  |
|  | Controls are collected (Automated) |  |  |
| 4.1.7 | Ensure login and logout events are collected (Automated) |  |  |
| 4.1.8 | Ensure session initiation information is collected |  |  |
|  | (Automated) |  |  |
| 4.1.9 | Ensure discretionary access control permission |  |  |
|  | modification events are collected (Automated) |  |  |
| 4.1.10 | Ensure unsuccessful unauthorized file access attempts are |  |  |
|  | collected (Automated) |  |  |
| 4.1.11 | Ensure use of privileged commands is collected |  |  |
|  | (Automated) |  |  |
| 4.1.12 | Ensure successful file system mounts are collected |  |  |
|  | (Automated) |  |  |
| 4.1.13 | Ensure file deletion events by users are collected |  |  |
|  | (Automated) |  |  |
| 4.1.14 | Ensure changes to system administration scope (sudoers) is |  |  |
|  | collected (Automated) |  |  |
| 4.1.15 | Ensure system administrator actions (sudolog) are collected |  |  |
|  | (Automated) |  |  |
| 4.1.16 | Ensure kernel module loading and unloading is collected |  |  |
|  | (Automated) |  |  |
| 4.1.17 | Ensure the audit configuration is immutable (Automated) |  |  |
| **4.2** | **Configure Logging** |  |  |
| **4.2.1** | **Configure rsyslog** |  |  |
| 4.2.1.1 | Ensure rsyslog is installed (Automated) |  |  |
| 4.2.1.2 | Ensure rsyslog Service is enabled and running (Automated) |  |  |
| 4.2.1.3 | Ensure rsyslog default file permissions configured |  |  |
|  | (Automated) |  |  |
| 4.2.1.4 | Ensure logging is configured (Manual) |  |  |
| 4.2.1.5 | Ensure rsyslog is configured to send logs to a remote log |  |  |
|  | host (Automated) |  |  |
| 4.2.1.6 | Ensure remote rsyslog messages are only accepted on |  |  |
|  | designated log hosts. (Manual) |  |  |
| **4.2.2** | **Configure journald** |  |  |
| 4.2.2.1 | Ensure journald is configured to send logs to rsyslog |  |  |
|  | (Automated) |  |  |
| 4.2.2.2 | Ensure journald is configured to compress large log files |  |  |
|  | (Automated) |  |  |
| 4.2.2.3 | Ensure journald is configured to write logfiles to persistent |  |  |
|  | disk (Automated) |  |  |
| 4.2.3 | Ensure permissions on all logfiles are configured |  |  |
|  | (Automated) |  |  |
| 4.2.4 | Ensure logrotate is configured (Manual) |  |  |
| **5** | **Access, Authentication and Authorization** |  |  |
| **5.1** | **Configure time-based job schedulers** |  |  |



530 | P a g e

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 5.1.1 | Ensure cron daemon is enabled and running (Automated) |  |  |  |
|  | 5.1.2 | Ensure permissions on /etc/crontab are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.1.3 | Ensure permissions on /etc/cron.hourly are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.1.4 | Ensure permissions on /etc/cron.daily are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.1.5 | Ensure permissions on /etc/cron.weekly are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.1.6 | Ensure permissions on /etc/cron.monthly are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.1.7 | Ensure permissions on /etc/cron.d are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.1.8 | Ensure cron is restricted to authorized users (Automated) |  |  |  |
|  | 5.1.9 | Ensure at is restricted to authorized users (Automated) |  |  |  |
|  | **5.2** | **Configure SSH Server** |  |  |  |
|  | 5.2.1 | Ensure permissions on /etc/ssh/sshd\_config are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.2.2 | Ensure permissions on SSH private host key files are |  |  |  |
|  |  | configured (Automated) |  |  |  |
|  | 5.2.3 | Ensure permissions on SSH public host key files are |  |  |  |
|  |  | configured (Automated) |  |  |  |
|  | 5.2.4 | Ensure SSH access is limited (Automated) |  |  |  |
|  | 5.2.5 | Ensure SSH LogLevel is appropriate (Automated) |  |  |  |
|  | 5.2.6 | Ensure SSH X11 forwarding is disabled (Automated) |  |  |  |
|  | 5.2.7 | Ensure SSH MaxAuthTries is set to 4 or less (Automated) |  |  |  |
|  | 5.2.8 | Ensure SSH IgnoreRhosts is enabled (Automated) |  |  |  |
|  | 5.2.9 | Ensure SSH HostbasedAuthentication is disabled |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.2.10 | Ensure SSH root login is disabled (Automated) |  |  |  |
|  | 5.2.11 | Ensure SSH PermitEmptyPasswords is disabled |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.2.12 | Ensure SSH PermitUserEnvironment is disabled |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.2.13 | Ensure only strong Ciphers are used (Automated) |  |  |  |
|  | 5.2.14 | Ensure only strong MAC algorithms are used (Automated) |  |  |  |
|  | 5.2.15 | Ensure only strong Key Exchange algorithms are used |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.2.16 | Ensure SSH Idle Timeout Interval is configured (Automated) |  |  |  |
|  | 5.2.17 | Ensure SSH LoginGraceTime is set to one minute or less |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.2.18 | Ensure SSH warning banner is configured (Automated) |  |  |  |
|  | 5.2.19 | Ensure SSH PAM is enabled (Automated) |  |  |  |
|  | 5.2.20 | Ensure SSH AllowTcpForwarding is disabled (Automated) |  |  |  |
|  | 5.2.21 | Ensure SSH MaxStartups is configured (Automated) |  |  |  |
|  |  |  |  |  |  |

531 | P a g e

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 5.2.22 | Ensure SSH MaxSessions is limited (Automated) |  |  |  |
|  | **5.3** | **Configure PAM** |  |  |  |
|  | 5.3.1 | Ensure password creation requirements are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.3.2 | Ensure lockout for failed password attempts is configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.3.3 | Ensure password reuse is limited (Automated) |  |  |  |
|  | **5.4** | **User Accounts and Environment** |  |  |  |
|  | **5.4.1** | **Set Shadow Password Suite Parameters** |  |  |  |
|  | 5.4.1.1 | Ensure password hashing algorithm is SHA-512 |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.4.1.2 | Ensure password expiration is 365 days or less (Automated) |  |  |  |
|  | 5.4.1.3 | Ensure minimum days between password changes is |  |  |  |
|  |  | configured (Automated) |  |  |  |
|  | 5.4.1.4 | Ensure password expiration warning days is 7 or more |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.4.1.5 | Ensure inactive password lock is 30 days or less |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.4.1.6 | Ensure all users last password change date is in the past |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.4.2 | Ensure system accounts are secured (Automated) |  |  |  |
|  | 5.4.3 | Ensure default group for the root account is GID 0 |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 5.4.4 | Ensure default user shell timeout is configured (Automated) |  |  |  |
|  | 5.4.5 | Ensure default user umask is configured (Automated) |  |  |  |
|  | 5.5 | Ensure root login is restricted to system console (Manual) |  |  |  |
|  | 5.6 | Ensure access to the su command is restricted (Automated) |  |  |  |
|  | **6** | **System Maintenance** |  |  |  |
|  | **6.1** | **System File Permissions** |  |  |  |
|  | 6.1.1 | Audit system file permissions (Manual) |  |  |  |
|  | 6.1.2 | Ensure permissions on /etc/passwd are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 6.1.3 | Ensure permissions on /etc/shadow are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 6.1.4 | Ensure permissions on /etc/group are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 6.1.5 | Ensure permissions on /etc/passwd- are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 6.1.6 | Ensure permissions on /etc/shadow- are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 6.1.7 | Ensure permissions on /etc/group- are configured |  |  |  |
|  |  | (Automated) |  |  |  |
|  | 6.1.8 | Ensure no world writable files exist (Automated) |  |  |  |
|  | 6.1.9 | Ensure no unowned files or directories exist (Automated) |  |  |  |
|  | 6.1.10 | Ensure no ungrouped files or directories exist (Automated) |  |  |  |
|  |  |  |  |  |  |

532 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 6.1.11 | Audit SUID executables (Manual) |  |  |
| 6.1.12 | Audit SGID executables (Manual) |  |  |
| **6.2** | **User and Group Settings** |  |  |
| 6.2.1 | Ensure accounts in /etc/passwd use shadowed passwords |  |  |
|  | (Automated) |  |  |
| 6.2.2 | Ensure /etc/shadow password fields are not empty |  |  |
|  | (Automated) |  |  |
| 6.2.3 | Ensure root is the only UID 0 account (Automated) |  |  |
| 6.2.4 | Ensure root PATH Integrity (Automated) |  |  |
| 6.2.5 | Ensure all users' home directories exist (Automated) |  |  |
| 6.2.6 | Ensure users' home directories permissions are 750 or |  |  |
|  | more restrictive (Automated) |  |  |
| 6.2.7 | Ensure users own their home directories (Automated) |  |  |
| 6.2.8 | Ensure users' dot files are not group or world writable |  |  |
|  | (Automated) |  |  |
| 6.2.9 | Ensure no users have .forward files (Automated) |  |  |
| 6.2.10 | Ensure no users have .netrc files (Automated) |  |  |
| 6.2.11 | Ensure users' .netrc Files are not group or world accessible |  |  |
|  | (Automated) |  |  |
| 6.2.12 | Ensure no users have .rhosts files (Automated) |  |  |
| 6.2.13 | Ensure all groups in /etc/passwd exist in /etc/group |  |  |
|  | (Automated) |  |  |
| 6.2.14 | Ensure no duplicate UIDs exist (Automated) |  |  |
| 6.2.15 | Ensure no duplicate GIDs exist (Automated) |  |  |
| 6.2.16 | Ensure no duplicate user names exist (Automated) |  |  |
| 6.2.17 | Ensure no duplicate group names exist (Automated) |  |  |
| 6.2.18 | Ensure shadow group is empty (Automated) |  |  |



533 | P a g e

**Appendix: CIS Controls v7 IG 1 Mapped Recommendations**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Recommendation** | **Set** | |
|  |  | **Correctly** | |
|  |  | Yes | No |
| 1.1.1.1 | Ensure mounting of squashfs filesystems is disabled |  |  |
| 1.1.1.2 | Ensure mounting of udf filesystems is disabled |  |  |
| 1.1.1.3 | Ensure mounting of FAT filesystems is limited |  |  |
| 1.1.2 | Ensure /tmp is configured |  |  |
| 1.1.3 | Ensure noexec option set on /tmp partition |  |  |
| 1.1.4 | Ensure nodev option set on /tmp partition |  |  |
| 1.1.5 | Ensure nosuid option set on /tmp partition |  |  |
| 1.1.6 | Ensure /dev/shm is configured |  |  |
| 1.1.7 | Ensure noexec option set on /dev/shm partition |  |  |
| 1.1.8 | Ensure nodev option set on /dev/shm partition |  |  |
| 1.1.9 | Ensure nosuid option set on /dev/shm partition |  |  |
| 1.1.10 | Ensure separate partition exists for /var |  |  |
| 1.1.11 | Ensure separate partition exists for /var/tmp |  |  |
| 1.1.12 | Ensure noexec option set on /var/tmp partition |  |  |
| 1.1.13 | Ensure nodev option set on /var/tmp partition |  |  |
| 1.1.14 | Ensure nosuid option set on /var/tmp partition |  |  |
| 1.1.17 | Ensure separate partition exists for /home |  |  |
| 1.1.18 | Ensure nodev option set on /home partition |  |  |
| 1.1.19 | Ensure noexec option set on removable media partitions |  |  |
| 1.1.20 | Ensure nodev option set on removable media partitions |  |  |
| 1.1.21 | Ensure nosuid option set on removable media partitions |  |  |
| 1.1.22 | Ensure sticky bit is set on all world-writable directories |  |  |
| 1.1.23 | Disable Automounting |  |  |
| 1.2.1 | Ensure GPG keys are configured |  |  |
| 1.2.2 | Ensure package manager repositories are configured |  |  |
| 1.2.3 | Ensure gpgcheck is globally activated |  |  |
| 1.5.1 | Ensure bootloader password is set |  |  |
| 1.5.2 | Ensure permissions on bootloader config are configured |  |  |
| 1.5.3 | Ensure authentication required for single user mode |  |  |
| 1.6.1 | Ensure core dumps are restricted |  |  |
| 1.7.1.1 | Ensure AppArmor is installed |  |  |
| 1.7.1.2 | Ensure AppArmor is enabled in the bootloader |  |  |
|  | configuration |  |  |
| 1.7.1.3 | Ensure all AppArmor Profiles are in enforce or complain |  |  |
|  | mode |  |  |
| 1.7.1.4 | Ensure all AppArmor Profiles are enforcing |  |  |
| 1.8.1.1 | Ensure message of the day is configured properly |  |  |



534 | P a g e

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1.8.1.2 | Ensure local login warning banner is configured properly |  |  |  |  |
|  | 1.8.1.3 | Ensure remote login warning banner is configured properly |  |  |  |  |
|  | 1.8.1.4 | Ensure permissions on /etc/motd are configured |  |  |  |  |
|  | 1.8.1.5 | Ensure permissions on /etc/issue are configured |  |  |  |  |
|  | 1.8.1.6 | Ensure permissions on /etc/issue.net are configured |  |  |  |  |
|  | 1.9 | Ensure updates, patches, and additional security software |  |  |  |  |
|  |  | are installed |  |  |  |  |
|  | 1.10 | Ensure GDM is removed or login is configured |  |  |  |  |
|  | 2.1.1 | Ensure xinetd is not installed |  |  |  |  |
|  | 2.2.2 | Ensure X11 Server components are not installed |  |  |  |  |
|  | 2.2.15 | Ensure net-snmp is not installed |  |  |  |  |
|  | 2.2.18 | Ensure NIS server is not installed |  |  |  |  |
|  | 2.2.19 | Ensure telnet-server is not installed |  |  |  |  |
|  | 2.3.1 | Ensure NIS Client is not installed |  |  |  |  |
|  | 2.3.2 | Ensure rsh client is not installed |  |  |  |  |
|  | 2.3.3 | Ensure talk client is not installed |  |  |  |  |
|  | 2.3.4 | Ensure telnet client is not installed |  |  |  |  |
|  | 2.3.5 | Ensure LDAP client is not installed |  |  |  |  |
|  | 3.1.1 | Disable IPv6 |  |  |  |  |
|  | 3.2.1 | Ensure IP forwarding is disabled |  |  |  |  |
|  | 3.2.2 | Ensure packet redirect sending is disabled |  |  |  |  |
|  | 3.3.1 | Ensure source routed packets are not accepted |  |  |  |  |
|  | 3.3.2 | Ensure ICMP redirects are not accepted |  |  |  |  |
|  | 3.3.3 | Ensure secure ICMP redirects are not accepted |  |  |  |  |
|  | 3.3.4 | Ensure suspicious packets are logged |  |  |  |  |
|  | 3.3.5 | Ensure broadcast ICMP requests are ignored |  |  |  |  |
|  | 3.3.6 | Ensure bogus ICMP responses are ignored |  |  |  |  |
|  | 3.3.7 | Ensure Reverse Path Filtering is enabled |  |  |  |  |
|  | 3.3.8 | Ensure TCP SYN Cookies is enabled |  |  |  |  |
|  | 3.3.9 | Ensure IPv6 router advertisements are not accepted |  |  |  |  |
|  | 3.5.1.1 | Ensure FirewallD is installed |  |  |  |  |
|  | 3.5.1.2 | Ensure nftables is not installed or stopped and masked |  |  |  |  |
|  | 3.5.1.3 | Ensure firewalld service is enabled and running |  |  |  |  |
|  | 3.5.1.4 | Ensure default zone is set |  |  |  |  |
|  | 3.5.1.5 | Ensure network interfaces are assigned to appropriate zone |  |  |  |  |
|  | 3.5.1.6 | Ensure unnecessary services and ports are not accepted |  |  |  |  |
|  | 3.5.2.1 | Ensure nftables is installed |  |  |  |  |
|  | 3.5.2.2 | Ensure firewalld is not installed or stopped and masked |  |  |  |  |
|  | 3.5.2.3 | Ensure iptables are flushed |  |  |  |  |
|  | 3.5.2.4 | Ensure a table exists |  |  |  |  |
|  | 3.5.2.5 | Ensure base chains exist |  |  |  |  |
|  | 3.5.2.6 | Ensure loopback traffic is configured |  |  |  |  |
|  | 3.5.2.7 | Ensure outbound and established connections are |  |  |  |  |
|  |  | configured |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  | 535 | P a g e | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 3.5.2.8 | Ensure default deny firewall policy |  |  |
| 3.5.2.9 | Ensure nftables service is enabled |  |  |
| 3.5.2.10 | Ensure nftables rules are permanent |  |  |
| 3.5.3.1.1 | Ensure iptables package is installed |  |  |
| 3.5.3.1.2 | Ensure nftables is not installed |  |  |
| 3.5.3.1.3 | Ensure firewalld is not installed or stopped and masked |  |  |
| 3.5.3.2.1 | Ensure default deny firewall policy |  |  |
| 3.5.3.2.2 | Ensure loopback traffic is configured |  |  |
| 3.5.3.2.3 | Ensure outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.3.2.4 | Ensure firewall rules exist for all open ports |  |  |
| 3.5.3.3.1 | Ensure IPv6 default deny firewall policy |  |  |
| 3.5.3.3.2 | Ensure IPv6 loopback traffic is configured |  |  |
| 3.5.3.3.3 | Ensure IPv6 outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.3.3.4 | Ensure IPv6 firewall rules exist for all open ports |  |  |
| 4.1.1.1 | Ensure auditd is installed |  |  |
| 4.1.1.2 | Ensure auditd service is enabled and running |  |  |
| 4.1.1.3 | Ensure auditing for processes that start prior to auditd is |  |  |
|  | enabled |  |  |
| 4.1.2.2 | Ensure audit logs are not automatically deleted |  |  |
| 4.1.2.3 | Ensure system is disabled when audit logs are full |  |  |
| 4.1.2.4 | Ensure audit\_backlog\_limit is sufficient |  |  |
| 4.1.5 | Ensure events that modify the system's network |  |  |
|  | environment are collected |  |  |
| 4.1.7 | Ensure login and logout events are collected |  |  |
| 4.1.8 | Ensure session initiation information is collected |  |  |
| 4.1.11 | Ensure use of privileged commands is collected |  |  |
| 4.1.12 | Ensure successful file system mounts are collected |  |  |
| 4.1.13 | Ensure file deletion events by users are collected |  |  |
| 4.1.16 | Ensure kernel module loading and unloading is collected |  |  |
| 4.1.17 | Ensure the audit configuration is immutable |  |  |
| 4.2.1.1 | Ensure rsyslog is installed |  |  |
| 4.2.1.2 | Ensure rsyslog Service is enabled and running |  |  |
| 4.2.1.3 | Ensure rsyslog default file permissions configured |  |  |
| 4.2.1.4 | Ensure logging is configured |  |  |
| 4.2.2.3 | Ensure journald is configured to write logfiles to persistent |  |  |
|  | disk |  |  |
| 4.2.3 | Ensure permissions on all logfiles are configured |  |  |
| 5.1.1 | Ensure cron daemon is enabled and running |  |  |
| 5.1.2 | Ensure permissions on /etc/crontab are configured |  |  |
| 5.1.3 | Ensure permissions on /etc/cron.hourly are configured |  |  |
| 5.1.4 | Ensure permissions on /etc/cron.daily are configured |  |  |
| 5.1.5 | Ensure permissions on /etc/cron.weekly are configured |  |  |



536 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 5.1.6 | Ensure permissions on /etc/cron.monthly are configured |  |  |
| 5.1.7 | Ensure permissions on /etc/cron.d are configured |  |  |
| 5.2.1 | Ensure permissions on /etc/ssh/sshd\_config are configured |  |  |
| 5.2.2 | Ensure permissions on SSH private host key files are |  |  |
|  | configured |  |  |
| 5.2.3 | Ensure permissions on SSH public host key files are |  |  |
|  | configured |  |  |
| 5.2.4 | Ensure SSH access is limited |  |  |
| 5.2.5 | Ensure SSH LogLevel is appropriate |  |  |
| 5.2.10 | Ensure SSH root login is disabled |  |  |
| 5.2.12 | Ensure SSH PermitUserEnvironment is disabled |  |  |
| 5.2.16 | Ensure SSH Idle Timeout Interval is configured |  |  |
| 5.2.17 | Ensure SSH LoginGraceTime is set to one minute or less |  |  |
| 5.2.18 | Ensure SSH warning banner is configured |  |  |
| 5.2.19 | Ensure SSH PAM is enabled |  |  |
| 5.2.21 | Ensure SSH MaxStartups is configured |  |  |
| 5.2.22 | Ensure SSH MaxSessions is limited |  |  |
| 5.4.1.5 | Ensure inactive password lock is 30 days or less |  |  |
| 5.4.3 | Ensure default group for the root account is GID 0 |  |  |
| 5.4.4 | Ensure default user shell timeout is configured |  |  |
| 5.4.5 | Ensure default user umask is configured |  |  |
| 5.5 | Ensure root login is restricted to system console |  |  |
| 5.6 | Ensure access to the su command is restricted |  |  |
| 6.1.1 | Audit system file permissions |  |  |
| 6.1.2 | Ensure permissions on /etc/passwd are configured |  |  |
| 6.1.3 | Ensure permissions on /etc/shadow are configured |  |  |
| 6.1.4 | Ensure permissions on /etc/group are configured |  |  |
| 6.1.5 | Ensure permissions on /etc/passwd- are configured |  |  |
| 6.1.6 | Ensure permissions on /etc/shadow- are configured |  |  |
| 6.1.7 | Ensure permissions on /etc/group- are configured |  |  |
| 6.1.8 | Ensure no world writable files exist |  |  |
| 6.1.9 | Ensure no unowned files or directories exist |  |  |
| 6.1.10 | Ensure no ungrouped files or directories exist |  |  |
| 6.1.11 | Audit SUID executables |  |  |
| 6.1.12 | Audit SGID executables |  |  |
| 6.2.3 | Ensure root is the only UID 0 account |  |  |
| 6.2.4 | Ensure root PATH Integrity |  |  |
| 6.2.5 | Ensure all users' home directories exist |  |  |
| 6.2.6 | Ensure users' home directories permissions are 750 or |  |  |
|  | more restrictive |  |  |
| 6.2.7 | Ensure users own their home directories |  |  |
| 6.2.8 | Ensure users' dot files are not group or world writable |  |  |
| 6.2.9 | Ensure no users have .forward files |  |  |
| 6.2.11 | Ensure users' .netrc Files are not group or world accessible |  |  |



537 | P a g e

6.2.18

Ensure shadow group is empty



 

538 | P a g e

**Appendix: CIS Controls v7 IG 2 Mapped Recommendations**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Recommendation** | **Set** | |
|  |  | **Correctly** | |
|  |  | Yes | No |
| 1.1.1.1 | Ensure mounting of squashfs filesystems is disabled |  |  |
| 1.1.1.2 | Ensure mounting of udf filesystems is disabled |  |  |
| 1.1.1.3 | Ensure mounting of FAT filesystems is limited |  |  |
| 1.1.2 | Ensure /tmp is configured |  |  |
| 1.1.3 | Ensure noexec option set on /tmp partition |  |  |
| 1.1.4 | Ensure nodev option set on /tmp partition |  |  |
| 1.1.5 | Ensure nosuid option set on /tmp partition |  |  |
| 1.1.6 | Ensure /dev/shm is configured |  |  |
| 1.1.7 | Ensure noexec option set on /dev/shm partition |  |  |
| 1.1.8 | Ensure nodev option set on /dev/shm partition |  |  |
| 1.1.9 | Ensure nosuid option set on /dev/shm partition |  |  |
| 1.1.10 | Ensure separate partition exists for /var |  |  |
| 1.1.11 | Ensure separate partition exists for /var/tmp |  |  |
| 1.1.12 | Ensure noexec option set on /var/tmp partition |  |  |
| 1.1.13 | Ensure nodev option set on /var/tmp partition |  |  |
| 1.1.14 | Ensure nosuid option set on /var/tmp partition |  |  |
| 1.1.15 | Ensure separate partition exists for /var/log |  |  |
| 1.1.16 | Ensure separate partition exists for /var/log/audit |  |  |
| 1.1.17 | Ensure separate partition exists for /home |  |  |
| 1.1.18 | Ensure nodev option set on /home partition |  |  |
| 1.1.19 | Ensure noexec option set on removable media partitions |  |  |
| 1.1.20 | Ensure nodev option set on removable media partitions |  |  |
| 1.1.21 | Ensure nosuid option set on removable media partitions |  |  |
| 1.1.22 | Ensure sticky bit is set on all world-writable directories |  |  |
| 1.1.23 | Disable Automounting |  |  |
| 1.2.1 | Ensure GPG keys are configured |  |  |
| 1.2.2 | Ensure package manager repositories are configured |  |  |
| 1.2.3 | Ensure gpgcheck is globally activated |  |  |
| 1.3.3 | Ensure sudo log file exists |  |  |
| 1.5.1 | Ensure bootloader password is set |  |  |
| 1.5.2 | Ensure permissions on bootloader config are configured |  |  |
| 1.5.3 | Ensure authentication required for single user mode |  |  |
| 1.6.1 | Ensure core dumps are restricted |  |  |
| 1.6.2 | Ensure XD/NX support is enabled |  |  |
| 1.6.3 | Ensure address space layout randomization (ASLR) is |  |  |
|  | enabled |  |  |
| 1.7.1.1 | Ensure AppArmor is installed |  |  |



539 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 1.7.1.2 | Ensure AppArmor is enabled in the bootloader |  |  |
|  | configuration |  |  |
| 1.7.1.3 | Ensure all AppArmor Profiles are in enforce or complain |  |  |
|  | mode |  |  |
| 1.7.1.4 | Ensure all AppArmor Profiles are enforcing |  |  |
| 1.8.1.1 | Ensure message of the day is configured properly |  |  |
| 1.8.1.2 | Ensure local login warning banner is configured properly |  |  |
| 1.8.1.3 | Ensure remote login warning banner is configured properly |  |  |
| 1.8.1.4 | Ensure permissions on /etc/motd are configured |  |  |
| 1.8.1.5 | Ensure permissions on /etc/issue are configured |  |  |
| 1.8.1.6 | Ensure permissions on /etc/issue.net are configured |  |  |
| 1.9 | Ensure updates, patches, and additional security software |  |  |
|  | are installed |  |  |
| 1.10 | Ensure GDM is removed or login is configured |  |  |
| 2.1.1 | Ensure xinetd is not installed |  |  |
| 2.2.1.1 | Ensure time synchronization is in use |  |  |
| 2.2.1.2 | Ensure systemd-timesyncd is configured |  |  |
| 2.2.1.3 | Ensure chrony is configured |  |  |
| 2.2.2 | Ensure X11 Server components are not installed |  |  |
| 2.2.3 | Ensure Avahi Server is not installed |  |  |
| 2.2.4 | Ensure CUPS is not installed |  |  |
| 2.2.5 | Ensure DHCP Server is not installed |  |  |
| 2.2.6 | Ensure LDAP server is not installed |  |  |
| 2.2.7 | Ensure nfs-utils is not installed or the nfs-server service is |  |  |
|  | masked |  |  |
| 2.2.8 | Ensure rpcbind is not installed or the rpcbind services are |  |  |
|  | masked |  |  |
| 2.2.9 | Ensure DNS Server is not installed |  |  |
| 2.2.10 | Ensure FTP Server is not installed |  |  |
| 2.2.11 | Ensure HTTP server is not installed |  |  |
| 2.2.12 | Ensure IMAP and POP3 server is not installed |  |  |
| 2.2.13 | Ensure Samba is not installed |  |  |
| 2.2.14 | Ensure HTTP Proxy Server is not installed |  |  |
| 2.2.15 | Ensure net-snmp is not installed |  |  |
| 2.2.16 | Ensure mail transfer agent is configured for local-only mode |  |  |
| 2.2.17 | Ensure rsync is not installed or the rsyncd service is masked |  |  |
| 2.2.18 | Ensure NIS server is not installed |  |  |
| 2.2.19 | Ensure telnet-server is not installed |  |  |
| 2.3.1 | Ensure NIS Client is not installed |  |  |
| 2.3.2 | Ensure rsh client is not installed |  |  |
| 2.3.3 | Ensure talk client is not installed |  |  |
| 2.3.4 | Ensure telnet client is not installed |  |  |
| 2.3.5 | Ensure LDAP client is not installed |  |  |
| 2.4 | Ensure nonessential services are removed or masked |  |  |



540 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 3.1.1 | Disable IPv6 |  |  |
| 3.2.1 | Ensure IP forwarding is disabled |  |  |
| 3.2.2 | Ensure packet redirect sending is disabled |  |  |
| 3.3.1 | Ensure source routed packets are not accepted |  |  |
| 3.3.2 | Ensure ICMP redirects are not accepted |  |  |
| 3.3.3 | Ensure secure ICMP redirects are not accepted |  |  |
| 3.3.4 | Ensure suspicious packets are logged |  |  |
| 3.3.5 | Ensure broadcast ICMP requests are ignored |  |  |
| 3.3.6 | Ensure bogus ICMP responses are ignored |  |  |
| 3.3.7 | Ensure Reverse Path Filtering is enabled |  |  |
| 3.3.8 | Ensure TCP SYN Cookies is enabled |  |  |
| 3.3.9 | Ensure IPv6 router advertisements are not accepted |  |  |
| 3.4.1 | Ensure DCCP is disabled |  |  |
| 3.4.2 | Ensure SCTP is disabled |  |  |
| 3.5.1.1 | Ensure FirewallD is installed |  |  |
| 3.5.1.2 | Ensure nftables is not installed or stopped and masked |  |  |
| 3.5.1.3 | Ensure firewalld service is enabled and running |  |  |
| 3.5.1.4 | Ensure default zone is set |  |  |
| 3.5.1.5 | Ensure network interfaces are assigned to appropriate zone |  |  |
| 3.5.1.6 | Ensure unnecessary services and ports are not accepted |  |  |
| 3.5.2.1 | Ensure nftables is installed |  |  |
| 3.5.2.2 | Ensure firewalld is not installed or stopped and masked |  |  |
| 3.5.2.3 | Ensure iptables are flushed |  |  |
| 3.5.2.4 | Ensure a table exists |  |  |
| 3.5.2.5 | Ensure base chains exist |  |  |
| 3.5.2.6 | Ensure loopback traffic is configured |  |  |
| 3.5.2.7 | Ensure outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.2.8 | Ensure default deny firewall policy |  |  |
| 3.5.2.9 | Ensure nftables service is enabled |  |  |
| 3.5.2.10 | Ensure nftables rules are permanent |  |  |
| 3.5.3.1.1 | Ensure iptables package is installed |  |  |
| 3.5.3.1.2 | Ensure nftables is not installed |  |  |
| 3.5.3.1.3 | Ensure firewalld is not installed or stopped and masked |  |  |
| 3.5.3.2.1 | Ensure default deny firewall policy |  |  |
| 3.5.3.2.2 | Ensure loopback traffic is configured |  |  |
| 3.5.3.2.3 | Ensure outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.3.2.4 | Ensure firewall rules exist for all open ports |  |  |
| 3.5.3.3.1 | Ensure IPv6 default deny firewall policy |  |  |
| 3.5.3.3.2 | Ensure IPv6 loopback traffic is configured |  |  |
| 3.5.3.3.3 | Ensure IPv6 outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.3.3.4 | Ensure IPv6 firewall rules exist for all open ports |  |  |



541 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 4.1.1.1 | Ensure auditd is installed |  |  |
| 4.1.1.2 | Ensure auditd service is enabled and running |  |  |
| 4.1.1.3 | Ensure auditing for processes that start prior to auditd is |  |  |
|  | enabled |  |  |
| 4.1.2.1 | Ensure audit log storage size is configured |  |  |
| 4.1.2.2 | Ensure audit logs are not automatically deleted |  |  |
| 4.1.2.3 | Ensure system is disabled when audit logs are full |  |  |
| 4.1.2.4 | Ensure audit\_backlog\_limit is sufficient |  |  |
| 4.1.3 | Ensure events that modify date and time information are |  |  |
|  | collected |  |  |
| 4.1.4 | Ensure events that modify user/group information are |  |  |
|  | collected |  |  |
| 4.1.5 | Ensure events that modify the system's network |  |  |
|  | environment are collected |  |  |
| 4.1.6 | Ensure events that modify the system's Mandatory Access |  |  |
|  | Controls are collected |  |  |
| 4.1.7 | Ensure login and logout events are collected |  |  |
| 4.1.8 | Ensure session initiation information is collected |  |  |
| 4.1.9 | Ensure discretionary access control permission |  |  |
|  | modification events are collected |  |  |
| 4.1.11 | Ensure use of privileged commands is collected |  |  |
| 4.1.12 | Ensure successful file system mounts are collected |  |  |
| 4.1.13 | Ensure file deletion events by users are collected |  |  |
| 4.1.14 | Ensure changes to system administration scope (sudoers) is |  |  |
|  | collected |  |  |
| 4.1.15 | Ensure system administrator actions (sudolog) are collected |  |  |
| 4.1.16 | Ensure kernel module loading and unloading is collected |  |  |
| 4.1.17 | Ensure the audit configuration is immutable |  |  |
| 4.2.1.1 | Ensure rsyslog is installed |  |  |
| 4.2.1.2 | Ensure rsyslog Service is enabled and running |  |  |
| 4.2.1.3 | Ensure rsyslog default file permissions configured |  |  |
| 4.2.1.4 | Ensure logging is configured |  |  |
| 4.2.1.5 | Ensure rsyslog is configured to send logs to a remote log |  |  |
|  | host |  |  |
| 4.2.1.6 | Ensure remote rsyslog messages are only accepted on |  |  |
|  | designated log hosts. |  |  |
| 4.2.2.1 | Ensure journald is configured to send logs to rsyslog |  |  |
| 4.2.2.2 | Ensure journald is configured to compress large log files |  |  |
| 4.2.2.3 | Ensure journald is configured to write logfiles to persistent |  |  |
|  | disk |  |  |
| 4.2.3 | Ensure permissions on all logfiles are configured |  |  |
| 4.2.4 | Ensure logrotate is configured |  |  |
| 5.1.1 | Ensure cron daemon is enabled and running |  |  |
| 5.1.2 | Ensure permissions on /etc/crontab are configured |  |  |



542 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 5.1.3 | Ensure permissions on /etc/cron.hourly are configured |  |  |
| 5.1.4 | Ensure permissions on /etc/cron.daily are configured |  |  |
| 5.1.5 | Ensure permissions on /etc/cron.weekly are configured |  |  |
| 5.1.6 | Ensure permissions on /etc/cron.monthly are configured |  |  |
| 5.1.7 | Ensure permissions on /etc/cron.d are configured |  |  |
| 5.2.1 | Ensure permissions on /etc/ssh/sshd\_config are configured |  |  |
| 5.2.2 | Ensure permissions on SSH private host key files are |  |  |
|  | configured |  |  |
| 5.2.3 | Ensure permissions on SSH public host key files are |  |  |
|  | configured |  |  |
| 5.2.4 | Ensure SSH access is limited |  |  |
| 5.2.5 | Ensure SSH LogLevel is appropriate |  |  |
| 5.2.6 | Ensure SSH X11 forwarding is disabled |  |  |
| 5.2.8 | Ensure SSH IgnoreRhosts is enabled |  |  |
| 5.2.9 | Ensure SSH HostbasedAuthentication is disabled |  |  |
| 5.2.10 | Ensure SSH root login is disabled |  |  |
| 5.2.11 | Ensure SSH PermitEmptyPasswords is disabled |  |  |
| 5.2.12 | Ensure SSH PermitUserEnvironment is disabled |  |  |
| 5.2.13 | Ensure only strong Ciphers are used |  |  |
| 5.2.14 | Ensure only strong MAC algorithms are used |  |  |
| 5.2.15 | Ensure only strong Key Exchange algorithms are used |  |  |
| 5.2.16 | Ensure SSH Idle Timeout Interval is configured |  |  |
| 5.2.17 | Ensure SSH LoginGraceTime is set to one minute or less |  |  |
| 5.2.18 | Ensure SSH warning banner is configured |  |  |
| 5.2.19 | Ensure SSH PAM is enabled |  |  |
| 5.2.20 | Ensure SSH AllowTcpForwarding is disabled |  |  |
| 5.2.21 | Ensure SSH MaxStartups is configured |  |  |
| 5.2.22 | Ensure SSH MaxSessions is limited |  |  |
| 5.3.1 | Ensure password creation requirements are configured |  |  |
| 5.3.2 | Ensure lockout for failed password attempts is configured |  |  |
| 5.4.1.1 | Ensure password hashing algorithm is SHA-512 |  |  |
| 5.4.1.2 | Ensure password expiration is 365 days or less |  |  |
| 5.4.1.3 | Ensure minimum days between password changes is |  |  |
|  | configured |  |  |
| 5.4.1.4 | Ensure password expiration warning days is 7 or more |  |  |
| 5.4.1.5 | Ensure inactive password lock is 30 days or less |  |  |
| 5.4.1.6 | Ensure all users last password change date is in the past |  |  |
| 5.4.3 | Ensure default group for the root account is GID 0 |  |  |
| 5.4.4 | Ensure default user shell timeout is configured |  |  |
| 5.4.5 | Ensure default user umask is configured |  |  |
| 5.5 | Ensure root login is restricted to system console |  |  |
| 5.6 | Ensure access to the su command is restricted |  |  |
| 6.1.1 | Audit system file permissions |  |  |
| 6.1.2 | Ensure permissions on /etc/passwd are configured |  |  |



543 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 6.1.3 | Ensure permissions on /etc/shadow are configured |  |  |
| 6.1.4 | Ensure permissions on /etc/group are configured |  |  |
| 6.1.5 | Ensure permissions on /etc/passwd- are configured |  |  |
| 6.1.6 | Ensure permissions on /etc/shadow- are configured |  |  |
| 6.1.7 | Ensure permissions on /etc/group- are configured |  |  |
| 6.1.8 | Ensure no world writable files exist |  |  |
| 6.1.9 | Ensure no unowned files or directories exist |  |  |
| 6.1.10 | Ensure no ungrouped files or directories exist |  |  |
| 6.1.11 | Audit SUID executables |  |  |
| 6.1.12 | Audit SGID executables |  |  |
| 6.2.1 | Ensure accounts in /etc/passwd use shadowed passwords |  |  |
| 6.2.2 | Ensure /etc/shadow password fields are not empty |  |  |
| 6.2.3 | Ensure root is the only UID 0 account |  |  |
| 6.2.4 | Ensure root PATH Integrity |  |  |
| 6.2.5 | Ensure all users' home directories exist |  |  |
| 6.2.6 | Ensure users' home directories permissions are 750 or |  |  |
|  | more restrictive |  |  |
| 6.2.7 | Ensure users own their home directories |  |  |
| 6.2.8 | Ensure users' dot files are not group or world writable |  |  |
| 6.2.9 | Ensure no users have .forward files |  |  |
| 6.2.10 | Ensure no users have .netrc files |  |  |
| 6.2.11 | Ensure users' .netrc Files are not group or world accessible |  |  |
| 6.2.12 | Ensure no users have .rhosts files |  |  |
| 6.2.18 | Ensure shadow group is empty |  |  |



544 | P a g e

**Appendix: CIS Controls v7 IG 3 Mapped Recommendations**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Recommendation** | **Set** | |
|  |  | **Correctly** | |
|  |  | Yes | No |
| 1.1.1.1 | Ensure mounting of squashfs filesystems is disabled |  |  |
| 1.1.1.2 | Ensure mounting of udf filesystems is disabled |  |  |
| 1.1.1.3 | Ensure mounting of FAT filesystems is limited |  |  |
| 1.1.2 | Ensure /tmp is configured |  |  |
| 1.1.3 | Ensure noexec option set on /tmp partition |  |  |
| 1.1.4 | Ensure nodev option set on /tmp partition |  |  |
| 1.1.5 | Ensure nosuid option set on /tmp partition |  |  |
| 1.1.6 | Ensure /dev/shm is configured |  |  |
| 1.1.7 | Ensure noexec option set on /dev/shm partition |  |  |
| 1.1.8 | Ensure nodev option set on /dev/shm partition |  |  |
| 1.1.9 | Ensure nosuid option set on /dev/shm partition |  |  |
| 1.1.10 | Ensure separate partition exists for /var |  |  |
| 1.1.11 | Ensure separate partition exists for /var/tmp |  |  |
| 1.1.12 | Ensure noexec option set on /var/tmp partition |  |  |
| 1.1.13 | Ensure nodev option set on /var/tmp partition |  |  |
| 1.1.14 | Ensure nosuid option set on /var/tmp partition |  |  |
| 1.1.15 | Ensure separate partition exists for /var/log |  |  |
| 1.1.16 | Ensure separate partition exists for /var/log/audit |  |  |
| 1.1.17 | Ensure separate partition exists for /home |  |  |
| 1.1.18 | Ensure nodev option set on /home partition |  |  |
| 1.1.19 | Ensure noexec option set on removable media partitions |  |  |
| 1.1.20 | Ensure nodev option set on removable media partitions |  |  |
| 1.1.21 | Ensure nosuid option set on removable media partitions |  |  |
| 1.1.22 | Ensure sticky bit is set on all world-writable directories |  |  |
| 1.1.23 | Disable Automounting |  |  |
| 1.2.1 | Ensure GPG keys are configured |  |  |
| 1.2.2 | Ensure package manager repositories are configured |  |  |
| 1.2.3 | Ensure gpgcheck is globally activated |  |  |
| 1.3.3 | Ensure sudo log file exists |  |  |
| 1.4.1 | Ensure AIDE is installed |  |  |
| 1.4.2 | Ensure filesystem integrity is regularly checked |  |  |
| 1.5.1 | Ensure bootloader password is set |  |  |
| 1.5.2 | Ensure permissions on bootloader config are configured |  |  |
| 1.5.3 | Ensure authentication required for single user mode |  |  |
| 1.6.1 | Ensure core dumps are restricted |  |  |
| 1.6.2 | Ensure XD/NX support is enabled |  |  |



545 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 1.6.3 | Ensure address space layout randomization (ASLR) is |  |  |
|  | enabled |  |  |
| 1.6.4 | Ensure prelink is disabled |  |  |
| 1.7.1.1 | Ensure AppArmor is installed |  |  |
| 1.7.1.2 | Ensure AppArmor is enabled in the bootloader |  |  |
|  | configuration |  |  |
| 1.7.1.3 | Ensure all AppArmor Profiles are in enforce or complain |  |  |
|  | mode |  |  |
| 1.7.1.4 | Ensure all AppArmor Profiles are enforcing |  |  |
| 1.8.1.1 | Ensure message of the day is configured properly |  |  |
| 1.8.1.2 | Ensure local login warning banner is configured properly |  |  |
| 1.8.1.3 | Ensure remote login warning banner is configured properly |  |  |
| 1.8.1.4 | Ensure permissions on /etc/motd are configured |  |  |
| 1.8.1.5 | Ensure permissions on /etc/issue are configured |  |  |
| 1.8.1.6 | Ensure permissions on /etc/issue.net are configured |  |  |
| 1.9 | Ensure updates, patches, and additional security software |  |  |
|  | are installed |  |  |
| 1.10 | Ensure GDM is removed or login is configured |  |  |
| 2.1.1 | Ensure xinetd is not installed |  |  |
| 2.2.1.1 | Ensure time synchronization is in use |  |  |
| 2.2.1.2 | Ensure systemd-timesyncd is configured |  |  |
| 2.2.1.3 | Ensure chrony is configured |  |  |
| 2.2.2 | Ensure X11 Server components are not installed |  |  |
| 2.2.3 | Ensure Avahi Server is not installed |  |  |
| 2.2.4 | Ensure CUPS is not installed |  |  |
| 2.2.5 | Ensure DHCP Server is not installed |  |  |
| 2.2.6 | Ensure LDAP server is not installed |  |  |
| 2.2.7 | Ensure nfs-utils is not installed or the nfs-server service is |  |  |
|  | masked |  |  |
| 2.2.8 | Ensure rpcbind is not installed or the rpcbind services are |  |  |
|  | masked |  |  |
| 2.2.9 | Ensure DNS Server is not installed |  |  |
| 2.2.10 | Ensure FTP Server is not installed |  |  |
| 2.2.11 | Ensure HTTP server is not installed |  |  |
| 2.2.12 | Ensure IMAP and POP3 server is not installed |  |  |
| 2.2.13 | Ensure Samba is not installed |  |  |
| 2.2.14 | Ensure HTTP Proxy Server is not installed |  |  |
| 2.2.15 | Ensure net-snmp is not installed |  |  |
| 2.2.16 | Ensure mail transfer agent is configured for local-only mode |  |  |
| 2.2.17 | Ensure rsync is not installed or the rsyncd service is masked |  |  |
| 2.2.18 | Ensure NIS server is not installed |  |  |
| 2.2.19 | Ensure telnet-server is not installed |  |  |
| 2.3.1 | Ensure NIS Client is not installed |  |  |
| 2.3.2 | Ensure rsh client is not installed |  |  |



546 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 2.3.3 | Ensure talk client is not installed |  |  |
| 2.3.4 | Ensure telnet client is not installed |  |  |
| 2.3.5 | Ensure LDAP client is not installed |  |  |
| 2.4 | Ensure nonessential services are removed or masked |  |  |
| 3.1.1 | Disable IPv6 |  |  |
| 3.1.2 | Ensure wireless interfaces are disabled |  |  |
| 3.2.1 | Ensure IP forwarding is disabled |  |  |
| 3.2.2 | Ensure packet redirect sending is disabled |  |  |
| 3.3.1 | Ensure source routed packets are not accepted |  |  |
| 3.3.2 | Ensure ICMP redirects are not accepted |  |  |
| 3.3.3 | Ensure secure ICMP redirects are not accepted |  |  |
| 3.3.4 | Ensure suspicious packets are logged |  |  |
| 3.3.5 | Ensure broadcast ICMP requests are ignored |  |  |
| 3.3.6 | Ensure bogus ICMP responses are ignored |  |  |
| 3.3.7 | Ensure Reverse Path Filtering is enabled |  |  |
| 3.3.8 | Ensure TCP SYN Cookies is enabled |  |  |
| 3.3.9 | Ensure IPv6 router advertisements are not accepted |  |  |
| 3.4.1 | Ensure DCCP is disabled |  |  |
| 3.4.2 | Ensure SCTP is disabled |  |  |
| 3.5.1.1 | Ensure FirewallD is installed |  |  |
| 3.5.1.2 | Ensure nftables is not installed or stopped and masked |  |  |
| 3.5.1.3 | Ensure firewalld service is enabled and running |  |  |
| 3.5.1.4 | Ensure default zone is set |  |  |
| 3.5.1.5 | Ensure network interfaces are assigned to appropriate zone |  |  |
| 3.5.1.6 | Ensure unnecessary services and ports are not accepted |  |  |
| 3.5.2.1 | Ensure nftables is installed |  |  |
| 3.5.2.2 | Ensure firewalld is not installed or stopped and masked |  |  |
| 3.5.2.3 | Ensure iptables are flushed |  |  |
| 3.5.2.4 | Ensure a table exists |  |  |
| 3.5.2.5 | Ensure base chains exist |  |  |
| 3.5.2.6 | Ensure loopback traffic is configured |  |  |
| 3.5.2.7 | Ensure outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.2.8 | Ensure default deny firewall policy |  |  |
| 3.5.2.9 | Ensure nftables service is enabled |  |  |
| 3.5.2.10 | Ensure nftables rules are permanent |  |  |
| 3.5.3.1.1 | Ensure iptables package is installed |  |  |
| 3.5.3.1.2 | Ensure nftables is not installed |  |  |
| 3.5.3.1.3 | Ensure firewalld is not installed or stopped and masked |  |  |
| 3.5.3.2.1 | Ensure default deny firewall policy |  |  |
| 3.5.3.2.2 | Ensure loopback traffic is configured |  |  |
| 3.5.3.2.3 | Ensure outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.3.2.4 | Ensure firewall rules exist for all open ports |  |  |



547 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 3.5.3.3.1 | Ensure IPv6 default deny firewall policy |  |  |
| 3.5.3.3.2 | Ensure IPv6 loopback traffic is configured |  |  |
| 3.5.3.3.3 | Ensure IPv6 outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.3.3.4 | Ensure IPv6 firewall rules exist for all open ports |  |  |
| 4.1.1.1 | Ensure auditd is installed |  |  |
| 4.1.1.2 | Ensure auditd service is enabled and running |  |  |
| 4.1.1.3 | Ensure auditing for processes that start prior to auditd is |  |  |
|  | enabled |  |  |
| 4.1.2.1 | Ensure audit log storage size is configured |  |  |
| 4.1.2.2 | Ensure audit logs are not automatically deleted |  |  |
| 4.1.2.3 | Ensure system is disabled when audit logs are full |  |  |
| 4.1.2.4 | Ensure audit\_backlog\_limit is sufficient |  |  |
| 4.1.3 | Ensure events that modify date and time information are |  |  |
|  | collected |  |  |
| 4.1.4 | Ensure events that modify user/group information are |  |  |
|  | collected |  |  |
| 4.1.5 | Ensure events that modify the system's network |  |  |
|  | environment are collected |  |  |
| 4.1.6 | Ensure events that modify the system's Mandatory Access |  |  |
|  | Controls are collected |  |  |
| 4.1.7 | Ensure login and logout events are collected |  |  |
| 4.1.8 | Ensure session initiation information is collected |  |  |
| 4.1.9 | Ensure discretionary access control permission |  |  |
|  | modification events are collected |  |  |
| 4.1.10 | Ensure unsuccessful unauthorized file access attempts are |  |  |
|  | collected |  |  |
| 4.1.11 | Ensure use of privileged commands is collected |  |  |
| 4.1.12 | Ensure successful file system mounts are collected |  |  |
| 4.1.13 | Ensure file deletion events by users are collected |  |  |
| 4.1.14 | Ensure changes to system administration scope (sudoers) is |  |  |
|  | collected |  |  |
| 4.1.15 | Ensure system administrator actions (sudolog) are collected |  |  |
| 4.1.16 | Ensure kernel module loading and unloading is collected |  |  |
| 4.1.17 | Ensure the audit configuration is immutable |  |  |
| 4.2.1.1 | Ensure rsyslog is installed |  |  |
| 4.2.1.2 | Ensure rsyslog Service is enabled and running |  |  |
| 4.2.1.3 | Ensure rsyslog default file permissions configured |  |  |
| 4.2.1.4 | Ensure logging is configured |  |  |
| 4.2.1.5 | Ensure rsyslog is configured to send logs to a remote log |  |  |
|  | host |  |  |
| 4.2.1.6 | Ensure remote rsyslog messages are only accepted on |  |  |
|  | designated log hosts. |  |  |
| 4.2.2.1 | Ensure journald is configured to send logs to rsyslog |  |  |



548 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 4.2.2.2 | Ensure journald is configured to compress large log files |  |  |
| 4.2.2.3 | Ensure journald is configured to write logfiles to persistent |  |  |
|  | disk |  |  |
| 4.2.3 | Ensure permissions on all logfiles are configured |  |  |
| 4.2.4 | Ensure logrotate is configured |  |  |
| 5.1.1 | Ensure cron daemon is enabled and running |  |  |
| 5.1.2 | Ensure permissions on /etc/crontab are configured |  |  |
| 5.1.3 | Ensure permissions on /etc/cron.hourly are configured |  |  |
| 5.1.4 | Ensure permissions on /etc/cron.daily are configured |  |  |
| 5.1.5 | Ensure permissions on /etc/cron.weekly are configured |  |  |
| 5.1.6 | Ensure permissions on /etc/cron.monthly are configured |  |  |
| 5.1.7 | Ensure permissions on /etc/cron.d are configured |  |  |
| 5.2.1 | Ensure permissions on /etc/ssh/sshd\_config are configured |  |  |
| 5.2.2 | Ensure permissions on SSH private host key files are |  |  |
|  | configured |  |  |
| 5.2.3 | Ensure permissions on SSH public host key files are |  |  |
|  | configured |  |  |
| 5.2.4 | Ensure SSH access is limited |  |  |
| 5.2.5 | Ensure SSH LogLevel is appropriate |  |  |
| 5.2.6 | Ensure SSH X11 forwarding is disabled |  |  |
| 5.2.7 | Ensure SSH MaxAuthTries is set to 4 or less |  |  |
| 5.2.8 | Ensure SSH IgnoreRhosts is enabled |  |  |
| 5.2.9 | Ensure SSH HostbasedAuthentication is disabled |  |  |
| 5.2.10 | Ensure SSH root login is disabled |  |  |
| 5.2.11 | Ensure SSH PermitEmptyPasswords is disabled |  |  |
| 5.2.12 | Ensure SSH PermitUserEnvironment is disabled |  |  |
| 5.2.13 | Ensure only strong Ciphers are used |  |  |
| 5.2.14 | Ensure only strong MAC algorithms are used |  |  |
| 5.2.15 | Ensure only strong Key Exchange algorithms are used |  |  |
| 5.2.16 | Ensure SSH Idle Timeout Interval is configured |  |  |
| 5.2.17 | Ensure SSH LoginGraceTime is set to one minute or less |  |  |
| 5.2.18 | Ensure SSH warning banner is configured |  |  |
| 5.2.19 | Ensure SSH PAM is enabled |  |  |
| 5.2.20 | Ensure SSH AllowTcpForwarding is disabled |  |  |
| 5.2.21 | Ensure SSH MaxStartups is configured |  |  |
| 5.2.22 | Ensure SSH MaxSessions is limited |  |  |
| 5.3.1 | Ensure password creation requirements are configured |  |  |
| 5.3.2 | Ensure lockout for failed password attempts is configured |  |  |
| 5.4.1.1 | Ensure password hashing algorithm is SHA-512 |  |  |
| 5.4.1.2 | Ensure password expiration is 365 days or less |  |  |
| 5.4.1.3 | Ensure minimum days between password changes is |  |  |
|  | configured |  |  |
| 5.4.1.4 | Ensure password expiration warning days is 7 or more |  |  |
| 5.4.1.5 | Ensure inactive password lock is 30 days or less |  |  |



549 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 5.4.1.6 | Ensure all users last password change date is in the past |  |  |
| 5.4.3 | Ensure default group for the root account is GID 0 |  |  |
| 5.4.4 | Ensure default user shell timeout is configured |  |  |
| 5.4.5 | Ensure default user umask is configured |  |  |
| 5.5 | Ensure root login is restricted to system console |  |  |
| 5.6 | Ensure access to the su command is restricted |  |  |
| 6.1.1 | Audit system file permissions |  |  |
| 6.1.2 | Ensure permissions on /etc/passwd are configured |  |  |
| 6.1.3 | Ensure permissions on /etc/shadow are configured |  |  |
| 6.1.4 | Ensure permissions on /etc/group are configured |  |  |
| 6.1.5 | Ensure permissions on /etc/passwd- are configured |  |  |
| 6.1.6 | Ensure permissions on /etc/shadow- are configured |  |  |
| 6.1.7 | Ensure permissions on /etc/group- are configured |  |  |
| 6.1.8 | Ensure no world writable files exist |  |  |
| 6.1.9 | Ensure no unowned files or directories exist |  |  |
| 6.1.10 | Ensure no ungrouped files or directories exist |  |  |
| 6.1.11 | Audit SUID executables |  |  |
| 6.1.12 | Audit SGID executables |  |  |
| 6.2.1 | Ensure accounts in /etc/passwd use shadowed passwords |  |  |
| 6.2.2 | Ensure /etc/shadow password fields are not empty |  |  |
| 6.2.3 | Ensure root is the only UID 0 account |  |  |
| 6.2.4 | Ensure root PATH Integrity |  |  |
| 6.2.5 | Ensure all users' home directories exist |  |  |
| 6.2.6 | Ensure users' home directories permissions are 750 or |  |  |
|  | more restrictive |  |  |
| 6.2.7 | Ensure users own their home directories |  |  |
| 6.2.8 | Ensure users' dot files are not group or world writable |  |  |
| 6.2.9 | Ensure no users have .forward files |  |  |
| 6.2.10 | Ensure no users have .netrc files |  |  |
| 6.2.11 | Ensure users' .netrc Files are not group or world accessible |  |  |
| 6.2.12 | Ensure no users have .rhosts files |  |  |
| 6.2.18 | Ensure shadow group is empty |  |  |



550 | P a g e

**Appendix: CIS Controls v8 IG 1 Mapped Recommendations**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Recommendation** | **Set** | |
|  |  | **Correctly** | |
|  |  | Yes | No |
| 1.1.1.1 | Ensure mounting of squashfs filesystems is disabled |  |  |
| 1.1.1.2 | Ensure mounting of udf filesystems is disabled |  |  |
| 1.1.1.3 | Ensure mounting of FAT filesystems is limited |  |  |
| 1.1.2 | Ensure /tmp is configured |  |  |
| 1.1.3 | Ensure noexec option set on /tmp partition |  |  |
| 1.1.4 | Ensure nodev option set on /tmp partition |  |  |
| 1.1.5 | Ensure nosuid option set on /tmp partition |  |  |
| 1.1.6 | Ensure /dev/shm is configured |  |  |
| 1.1.7 | Ensure noexec option set on /dev/shm partition |  |  |
| 1.1.8 | Ensure nodev option set on /dev/shm partition |  |  |
| 1.1.9 | Ensure nosuid option set on /dev/shm partition |  |  |
| 1.1.10 | Ensure separate partition exists for /var |  |  |
| 1.1.11 | Ensure separate partition exists for /var/tmp |  |  |
| 1.1.12 | Ensure noexec option set on /var/tmp partition |  |  |
| 1.1.13 | Ensure nodev option set on /var/tmp partition |  |  |
| 1.1.14 | Ensure nosuid option set on /var/tmp partition |  |  |
| 1.1.15 | Ensure separate partition exists for /var/log |  |  |
| 1.1.16 | Ensure separate partition exists for /var/log/audit |  |  |
| 1.1.17 | Ensure separate partition exists for /home |  |  |
| 1.1.18 | Ensure nodev option set on /home partition |  |  |
| 1.1.19 | Ensure noexec option set on removable media partitions |  |  |
| 1.1.20 | Ensure nodev option set on removable media partitions |  |  |
| 1.1.21 | Ensure nosuid option set on removable media partitions |  |  |
| 1.1.22 | Ensure sticky bit is set on all world-writable directories |  |  |
| 1.1.23 | Disable Automounting |  |  |
| 1.2.1 | Ensure GPG keys are configured |  |  |
| 1.2.2 | Ensure package manager repositories are configured |  |  |
| 1.2.3 | Ensure gpgcheck is globally activated |  |  |
| 1.3.1 | Ensure sudo is installed |  |  |
| 1.3.2 | Ensure sudo commands use pty |  |  |
| 1.5.1 | Ensure bootloader password is set |  |  |
| 1.5.2 | Ensure permissions on bootloader config are configured |  |  |
| 1.5.3 | Ensure authentication required for single user mode |  |  |
| 1.6.1 | Ensure core dumps are restricted |  |  |
| 1.6.4 | Ensure prelink is disabled |  |  |
| 1.7.1.1 | Ensure AppArmor is installed |  |  |



551 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 1.7.1.2 | Ensure AppArmor is enabled in the bootloader |  |  |
|  | configuration |  |  |
| 1.7.1.3 | Ensure all AppArmor Profiles are in enforce or complain |  |  |
|  | mode |  |  |
| 1.7.1.4 | Ensure all AppArmor Profiles are enforcing |  |  |
| 1.8.1.1 | Ensure message of the day is configured properly |  |  |
| 1.8.1.2 | Ensure local login warning banner is configured properly |  |  |
| 1.8.1.3 | Ensure remote login warning banner is configured properly |  |  |
| 1.8.1.4 | Ensure permissions on /etc/motd are configured |  |  |
| 1.8.1.5 | Ensure permissions on /etc/issue are configured |  |  |
| 1.8.1.6 | Ensure permissions on /etc/issue.net are configured |  |  |
| 1.9 | Ensure updates, patches, and additional security software |  |  |
|  | are installed |  |  |
| 1.10 | Ensure GDM is removed or login is configured |  |  |
| 3.2.1 | Ensure IP forwarding is disabled |  |  |
| 3.2.2 | Ensure packet redirect sending is disabled |  |  |
| 3.3.1 | Ensure source routed packets are not accepted |  |  |
| 3.3.2 | Ensure ICMP redirects are not accepted |  |  |
| 3.3.3 | Ensure secure ICMP redirects are not accepted |  |  |
| 3.3.5 | Ensure broadcast ICMP requests are ignored |  |  |
| 3.3.6 | Ensure bogus ICMP responses are ignored |  |  |
| 3.3.7 | Ensure Reverse Path Filtering is enabled |  |  |
| 3.3.8 | Ensure TCP SYN Cookies is enabled |  |  |
| 3.3.9 | Ensure IPv6 router advertisements are not accepted |  |  |
| 3.5.1.1 | Ensure FirewallD is installed |  |  |
| 3.5.1.2 | Ensure nftables is not installed or stopped and masked |  |  |
| 3.5.1.3 | Ensure firewalld service is enabled and running |  |  |
| 3.5.1.4 | Ensure default zone is set |  |  |
| 3.5.1.5 | Ensure network interfaces are assigned to appropriate zone |  |  |
| 3.5.1.6 | Ensure unnecessary services and ports are not accepted |  |  |
| 3.5.2.1 | Ensure nftables is installed |  |  |
| 3.5.2.2 | Ensure firewalld is not installed or stopped and masked |  |  |
| 3.5.2.3 | Ensure iptables are flushed |  |  |
| 3.5.2.4 | Ensure a table exists |  |  |
| 3.5.2.5 | Ensure base chains exist |  |  |
| 3.5.2.6 | Ensure loopback traffic is configured |  |  |
| 3.5.2.7 | Ensure outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.2.8 | Ensure default deny firewall policy |  |  |
| 3.5.2.9 | Ensure nftables service is enabled |  |  |
| 3.5.2.10 | Ensure nftables rules are permanent |  |  |
| 3.5.3.1.1 | Ensure iptables package is installed |  |  |
| 3.5.3.1.2 | Ensure nftables is not installed |  |  |
| 3.5.3.1.3 | Ensure firewalld is not installed or stopped and masked |  |  |



552 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 3.5.3.2.1 | Ensure default deny firewall policy |  |  |
| 3.5.3.2.2 | Ensure loopback traffic is configured |  |  |
| 3.5.3.2.3 | Ensure outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.3.2.4 | Ensure firewall rules exist for all open ports |  |  |
| 3.5.3.3.1 | Ensure IPv6 default deny firewall policy |  |  |
| 3.5.3.3.2 | Ensure IPv6 loopback traffic is configured |  |  |
| 3.5.3.3.3 | Ensure IPv6 outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.3.3.4 | Ensure IPv6 firewall rules exist for all open ports |  |  |
| 4.1.1.1 | Ensure auditd is installed |  |  |
| 4.1.1.2 | Ensure auditd service is enabled and running |  |  |
| 4.1.1.3 | Ensure auditing for processes that start prior to auditd is |  |  |
|  | enabled |  |  |
| 4.1.2.3 | Ensure system is disabled when audit logs are full |  |  |
| 4.1.2.4 | Ensure audit\_backlog\_limit is sufficient |  |  |
| 4.1.17 | Ensure the audit configuration is immutable |  |  |
| 4.2.1.1 | Ensure rsyslog is installed |  |  |
| 4.2.1.2 | Ensure rsyslog Service is enabled and running |  |  |
| 4.2.1.3 | Ensure rsyslog default file permissions configured |  |  |
| 4.2.1.4 | Ensure logging is configured |  |  |
| 4.2.1.6 | Ensure remote rsyslog messages are only accepted on |  |  |
|  | designated log hosts. |  |  |
| 4.2.2.3 | Ensure journald is configured to write logfiles to persistent |  |  |
|  | disk |  |  |
| 4.2.3 | Ensure permissions on all logfiles are configured |  |  |
| 5.1.1 | Ensure cron daemon is enabled and running |  |  |
| 5.1.2 | Ensure permissions on /etc/crontab are configured |  |  |
| 5.1.3 | Ensure permissions on /etc/cron.hourly are configured |  |  |
| 5.1.4 | Ensure permissions on /etc/cron.daily are configured |  |  |
| 5.1.5 | Ensure permissions on /etc/cron.weekly are configured |  |  |
| 5.1.6 | Ensure permissions on /etc/cron.monthly are configured |  |  |
| 5.1.7 | Ensure permissions on /etc/cron.d are configured |  |  |
| 5.1.8 | Ensure cron is restricted to authorized users |  |  |
| 5.1.9 | Ensure at is restricted to authorized users |  |  |
| 5.2.1 | Ensure permissions on /etc/ssh/sshd\_config are configured |  |  |
| 5.2.2 | Ensure permissions on SSH private host key files are |  |  |
|  | configured |  |  |
| 5.2.3 | Ensure permissions on SSH public host key files are |  |  |
|  | configured |  |  |
| 5.2.4 | Ensure SSH access is limited |  |  |
| 5.2.5 | Ensure SSH LogLevel is appropriate |  |  |
| 5.2.8 | Ensure SSH IgnoreRhosts is enabled |  |  |
| 5.2.9 | Ensure SSH HostbasedAuthentication is disabled |  |  |



553 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 5.2.10 | Ensure SSH root login is disabled |  |  |
| 5.2.11 | Ensure SSH PermitEmptyPasswords is disabled |  |  |
| 5.2.12 | Ensure SSH PermitUserEnvironment is disabled |  |  |
| 5.2.14 | Ensure only strong MAC algorithms are used |  |  |
| 5.2.15 | Ensure only strong Key Exchange algorithms are used |  |  |
| 5.2.16 | Ensure SSH Idle Timeout Interval is configured |  |  |
| 5.2.17 | Ensure SSH LoginGraceTime is set to one minute or less |  |  |
| 5.2.18 | Ensure SSH warning banner is configured |  |  |
| 5.2.19 | Ensure SSH PAM is enabled |  |  |
| 5.2.20 | Ensure SSH AllowTcpForwarding is disabled |  |  |
| 5.2.21 | Ensure SSH MaxStartups is configured |  |  |
| 5.2.22 | Ensure SSH MaxSessions is limited |  |  |
| 5.3.1 | Ensure password creation requirements are configured |  |  |
| 5.3.2 | Ensure lockout for failed password attempts is configured |  |  |
| 5.3.3 | Ensure password reuse is limited |  |  |
| 5.4.1.2 | Ensure password expiration is 365 days or less |  |  |
| 5.4.1.3 | Ensure minimum days between password changes is |  |  |
|  | configured |  |  |
| 5.4.1.4 | Ensure password expiration warning days is 7 or more |  |  |
| 5.4.1.5 | Ensure inactive password lock is 30 days or less |  |  |
| 5.4.1.6 | Ensure all users last password change date is in the past |  |  |
| 5.4.2 | Ensure system accounts are secured |  |  |
| 5.4.3 | Ensure default group for the root account is GID 0 |  |  |
| 5.4.4 | Ensure default user shell timeout is configured |  |  |
| 5.4.5 | Ensure default user umask is configured |  |  |
| 5.5 | Ensure root login is restricted to system console |  |  |
| 5.6 | Ensure access to the su command is restricted |  |  |
| 6.1.1 | Audit system file permissions |  |  |
| 6.1.2 | Ensure permissions on /etc/passwd are configured |  |  |
| 6.1.3 | Ensure permissions on /etc/shadow are configured |  |  |
| 6.1.4 | Ensure permissions on /etc/group are configured |  |  |
| 6.1.5 | Ensure permissions on /etc/passwd- are configured |  |  |
| 6.1.6 | Ensure permissions on /etc/shadow- are configured |  |  |
| 6.1.7 | Ensure permissions on /etc/group- are configured |  |  |
| 6.1.8 | Ensure no world writable files exist |  |  |
| 6.1.9 | Ensure no unowned files or directories exist |  |  |
| 6.1.10 | Ensure no ungrouped files or directories exist |  |  |
| 6.1.11 | Audit SUID executables |  |  |
| 6.1.12 | Audit SGID executables |  |  |
| 6.2.2 | Ensure /etc/shadow password fields are not empty |  |  |
| 6.2.3 | Ensure root is the only UID 0 account |  |  |
| 6.2.4 | Ensure root PATH Integrity |  |  |
| 6.2.5 | Ensure all users' home directories exist |  |  |



554 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 6.2.6 | Ensure users' home directories permissions are 750 or |  |  |
|  | more restrictive |  |  |
| 6.2.7 | Ensure users own their home directories |  |  |
| 6.2.8 | Ensure users' dot files are not group or world writable |  |  |
| 6.2.9 | Ensure no users have .forward files |  |  |
| 6.2.10 | Ensure no users have .netrc files |  |  |
| 6.2.11 | Ensure users' .netrc Files are not group or world accessible |  |  |
| 6.2.12 | Ensure no users have .rhosts files |  |  |
| 6.2.13 | Ensure all groups in /etc/passwd exist in /etc/group |  |  |
| 6.2.14 | Ensure no duplicate UIDs exist |  |  |
| 6.2.15 | Ensure no duplicate GIDs exist |  |  |
| 6.2.16 | Ensure no duplicate user names exist |  |  |
| 6.2.17 | Ensure no duplicate group names exist |  |  |
| 6.2.18 | Ensure shadow group is empty |  |  |



555 | P a g e

**Appendix: CIS Controls v8 IG 2 Mapped Recommendations**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Recommendation** | **Set** | |
|  |  | **Correctly** | |
|  |  | Yes | No |
| 1.1.1.1 | Ensure mounting of squashfs filesystems is disabled |  |  |
| 1.1.1.2 | Ensure mounting of udf filesystems is disabled |  |  |
| 1.1.1.3 | Ensure mounting of FAT filesystems is limited |  |  |
| 1.1.2 | Ensure /tmp is configured |  |  |
| 1.1.3 | Ensure noexec option set on /tmp partition |  |  |
| 1.1.4 | Ensure nodev option set on /tmp partition |  |  |
| 1.1.5 | Ensure nosuid option set on /tmp partition |  |  |
| 1.1.6 | Ensure /dev/shm is configured |  |  |
| 1.1.7 | Ensure noexec option set on /dev/shm partition |  |  |
| 1.1.8 | Ensure nodev option set on /dev/shm partition |  |  |
| 1.1.9 | Ensure nosuid option set on /dev/shm partition |  |  |
| 1.1.10 | Ensure separate partition exists for /var |  |  |
| 1.1.11 | Ensure separate partition exists for /var/tmp |  |  |
| 1.1.12 | Ensure noexec option set on /var/tmp partition |  |  |
| 1.1.13 | Ensure nodev option set on /var/tmp partition |  |  |
| 1.1.14 | Ensure nosuid option set on /var/tmp partition |  |  |
| 1.1.15 | Ensure separate partition exists for /var/log |  |  |
| 1.1.16 | Ensure separate partition exists for /var/log/audit |  |  |
| 1.1.17 | Ensure separate partition exists for /home |  |  |
| 1.1.18 | Ensure nodev option set on /home partition |  |  |
| 1.1.19 | Ensure noexec option set on removable media partitions |  |  |
| 1.1.20 | Ensure nodev option set on removable media partitions |  |  |
| 1.1.21 | Ensure nosuid option set on removable media partitions |  |  |
| 1.1.22 | Ensure sticky bit is set on all world-writable directories |  |  |
| 1.1.23 | Disable Automounting |  |  |
| 1.2.1 | Ensure GPG keys are configured |  |  |
| 1.2.2 | Ensure package manager repositories are configured |  |  |
| 1.2.3 | Ensure gpgcheck is globally activated |  |  |
| 1.3.1 | Ensure sudo is installed |  |  |
| 1.3.2 | Ensure sudo commands use pty |  |  |
| 1.3.3 | Ensure sudo log file exists |  |  |
| 1.5.1 | Ensure bootloader password is set |  |  |
| 1.5.2 | Ensure permissions on bootloader config are configured |  |  |
| 1.5.3 | Ensure authentication required for single user mode |  |  |
| 1.6.1 | Ensure core dumps are restricted |  |  |
| 1.6.2 | Ensure XD/NX support is enabled |  |  |



556 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 1.6.3 | Ensure address space layout randomization (ASLR) is |  |  |
|  | enabled |  |  |
| 1.6.4 | Ensure prelink is disabled |  |  |
| 1.7.1.1 | Ensure AppArmor is installed |  |  |
| 1.7.1.2 | Ensure AppArmor is enabled in the bootloader |  |  |
|  | configuration |  |  |
| 1.7.1.3 | Ensure all AppArmor Profiles are in enforce or complain |  |  |
|  | mode |  |  |
| 1.7.1.4 | Ensure all AppArmor Profiles are enforcing |  |  |
| 1.8.1.1 | Ensure message of the day is configured properly |  |  |
| 1.8.1.2 | Ensure local login warning banner is configured properly |  |  |
| 1.8.1.3 | Ensure remote login warning banner is configured properly |  |  |
| 1.8.1.4 | Ensure permissions on /etc/motd are configured |  |  |
| 1.8.1.5 | Ensure permissions on /etc/issue are configured |  |  |
| 1.8.1.6 | Ensure permissions on /etc/issue.net are configured |  |  |
| 1.9 | Ensure updates, patches, and additional security software |  |  |
|  | are installed |  |  |
| 1.10 | Ensure GDM is removed or login is configured |  |  |
| 2.1.1 | Ensure xinetd is not installed |  |  |
| 2.2.1.1 | Ensure time synchronization is in use |  |  |
| 2.2.1.2 | Ensure systemd-timesyncd is configured |  |  |
| 2.2.1.3 | Ensure chrony is configured |  |  |
| 2.2.2 | Ensure X11 Server components are not installed |  |  |
| 2.2.3 | Ensure Avahi Server is not installed |  |  |
| 2.2.4 | Ensure CUPS is not installed |  |  |
| 2.2.5 | Ensure DHCP Server is not installed |  |  |
| 2.2.6 | Ensure LDAP server is not installed |  |  |
| 2.2.7 | Ensure nfs-utils is not installed or the nfs-server service is |  |  |
|  | masked |  |  |
| 2.2.8 | Ensure rpcbind is not installed or the rpcbind services are |  |  |
|  | masked |  |  |
| 2.2.9 | Ensure DNS Server is not installed |  |  |
| 2.2.10 | Ensure FTP Server is not installed |  |  |
| 2.2.11 | Ensure HTTP server is not installed |  |  |
| 2.2.12 | Ensure IMAP and POP3 server is not installed |  |  |
| 2.2.13 | Ensure Samba is not installed |  |  |
| 2.2.14 | Ensure HTTP Proxy Server is not installed |  |  |
| 2.2.15 | Ensure net-snmp is not installed |  |  |
| 2.2.16 | Ensure mail transfer agent is configured for local-only mode |  |  |
| 2.2.17 | Ensure rsync is not installed or the rsyncd service is masked |  |  |
| 2.2.18 | Ensure NIS server is not installed |  |  |
| 2.2.19 | Ensure telnet-server is not installed |  |  |
| 2.3.1 | Ensure NIS Client is not installed |  |  |
| 2.3.2 | Ensure rsh client is not installed |  |  |



557 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 2.3.3 | Ensure talk client is not installed |  |  |
| 2.3.4 | Ensure telnet client is not installed |  |  |
| 2.3.5 | Ensure LDAP client is not installed |  |  |
| 2.4 | Ensure nonessential services are removed or masked |  |  |
| 3.1.1 | Disable IPv6 |  |  |
| 3.1.2 | Ensure wireless interfaces are disabled |  |  |
| 3.2.1 | Ensure IP forwarding is disabled |  |  |
| 3.2.2 | Ensure packet redirect sending is disabled |  |  |
| 3.3.1 | Ensure source routed packets are not accepted |  |  |
| 3.3.2 | Ensure ICMP redirects are not accepted |  |  |
| 3.3.3 | Ensure secure ICMP redirects are not accepted |  |  |
| 3.3.4 | Ensure suspicious packets are logged |  |  |
| 3.3.5 | Ensure broadcast ICMP requests are ignored |  |  |
| 3.3.6 | Ensure bogus ICMP responses are ignored |  |  |
| 3.3.7 | Ensure Reverse Path Filtering is enabled |  |  |
| 3.3.8 | Ensure TCP SYN Cookies is enabled |  |  |
| 3.3.9 | Ensure IPv6 router advertisements are not accepted |  |  |
| 3.4.1 | Ensure DCCP is disabled |  |  |
| 3.4.2 | Ensure SCTP is disabled |  |  |
| 3.5.1.1 | Ensure FirewallD is installed |  |  |
| 3.5.1.2 | Ensure nftables is not installed or stopped and masked |  |  |
| 3.5.1.3 | Ensure firewalld service is enabled and running |  |  |
| 3.5.1.4 | Ensure default zone is set |  |  |
| 3.5.1.5 | Ensure network interfaces are assigned to appropriate zone |  |  |
| 3.5.1.6 | Ensure unnecessary services and ports are not accepted |  |  |
| 3.5.2.1 | Ensure nftables is installed |  |  |
| 3.5.2.2 | Ensure firewalld is not installed or stopped and masked |  |  |
| 3.5.2.3 | Ensure iptables are flushed |  |  |
| 3.5.2.4 | Ensure a table exists |  |  |
| 3.5.2.5 | Ensure base chains exist |  |  |
| 3.5.2.6 | Ensure loopback traffic is configured |  |  |
| 3.5.2.7 | Ensure outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.2.8 | Ensure default deny firewall policy |  |  |
| 3.5.2.9 | Ensure nftables service is enabled |  |  |
| 3.5.2.10 | Ensure nftables rules are permanent |  |  |
| 3.5.3.1.1 | Ensure iptables package is installed |  |  |
| 3.5.3.1.2 | Ensure nftables is not installed |  |  |
| 3.5.3.1.3 | Ensure firewalld is not installed or stopped and masked |  |  |
| 3.5.3.2.1 | Ensure default deny firewall policy |  |  |
| 3.5.3.2.2 | Ensure loopback traffic is configured |  |  |
| 3.5.3.2.3 | Ensure outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.3.2.4 | Ensure firewall rules exist for all open ports |  |  |



558 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 3.5.3.3.1 | Ensure IPv6 default deny firewall policy |  |  |
| 3.5.3.3.2 | Ensure IPv6 loopback traffic is configured |  |  |
| 3.5.3.3.3 | Ensure IPv6 outbound and established connections are |  |  |
|  | configured |  |  |
| 3.5.3.3.4 | Ensure IPv6 firewall rules exist for all open ports |  |  |
| 4.1.1.1 | Ensure auditd is installed |  |  |
| 4.1.1.2 | Ensure auditd service is enabled and running |  |  |
| 4.1.1.3 | Ensure auditing for processes that start prior to auditd is |  |  |
|  | enabled |  |  |
| 4.1.2.1 | Ensure audit log storage size is configured |  |  |
| 4.1.2.2 | Ensure audit logs are not automatically deleted |  |  |
| 4.1.2.3 | Ensure system is disabled when audit logs are full |  |  |
| 4.1.2.4 | Ensure audit\_backlog\_limit is sufficient |  |  |
| 4.1.3 | Ensure events that modify date and time information are |  |  |
|  | collected |  |  |
| 4.1.4 | Ensure events that modify user/group information are |  |  |
|  | collected |  |  |
| 4.1.5 | Ensure events that modify the system's network |  |  |
|  | environment are collected |  |  |
| 4.1.6 | Ensure events that modify the system's Mandatory Access |  |  |
|  | Controls are collected |  |  |
| 4.1.7 | Ensure login and logout events are collected |  |  |
| 4.1.8 | Ensure session initiation information is collected |  |  |
| 4.1.9 | Ensure discretionary access control permission |  |  |
|  | modification events are collected |  |  |
| 4.1.10 | Ensure unsuccessful unauthorized file access attempts are |  |  |
|  | collected |  |  |
| 4.1.11 | Ensure use of privileged commands is collected |  |  |
| 4.1.12 | Ensure successful file system mounts are collected |  |  |
| 4.1.13 | Ensure file deletion events by users are collected |  |  |
| 4.1.14 | Ensure changes to system administration scope (sudoers) is |  |  |
|  | collected |  |  |
| 4.1.15 | Ensure system administrator actions (sudolog) are collected |  |  |
| 4.1.16 | Ensure kernel module loading and unloading is collected |  |  |
| 4.1.17 | Ensure the audit configuration is immutable |  |  |
| 4.2.1.1 | Ensure rsyslog is installed |  |  |
| 4.2.1.2 | Ensure rsyslog Service is enabled and running |  |  |
| 4.2.1.3 | Ensure rsyslog default file permissions configured |  |  |
| 4.2.1.4 | Ensure logging is configured |  |  |
| 4.2.1.5 | Ensure rsyslog is configured to send logs to a remote log |  |  |
|  | host |  |  |
| 4.2.1.6 | Ensure remote rsyslog messages are only accepted on |  |  |
|  | designated log hosts. |  |  |
| 4.2.2.1 | Ensure journald is configured to send logs to rsyslog |  |  |



559 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 4.2.2.2 | Ensure journald is configured to compress large log files |  |  |
| 4.2.2.3 | Ensure journald is configured to write logfiles to persistent |  |  |
|  | disk |  |  |
| 4.2.3 | Ensure permissions on all logfiles are configured |  |  |
| 4.2.4 | Ensure logrotate is configured |  |  |
| 5.1.1 | Ensure cron daemon is enabled and running |  |  |
| 5.1.2 | Ensure permissions on /etc/crontab are configured |  |  |
| 5.1.3 | Ensure permissions on /etc/cron.hourly are configured |  |  |
| 5.1.4 | Ensure permissions on /etc/cron.daily are configured |  |  |
| 5.1.5 | Ensure permissions on /etc/cron.weekly are configured |  |  |
| 5.1.6 | Ensure permissions on /etc/cron.monthly are configured |  |  |
| 5.1.7 | Ensure permissions on /etc/cron.d are configured |  |  |
| 5.1.8 | Ensure cron is restricted to authorized users |  |  |
| 5.1.9 | Ensure at is restricted to authorized users |  |  |
| 5.2.1 | Ensure permissions on /etc/ssh/sshd\_config are configured |  |  |
| 5.2.2 | Ensure permissions on SSH private host key files are |  |  |
|  | configured |  |  |
| 5.2.3 | Ensure permissions on SSH public host key files are |  |  |
|  | configured |  |  |
| 5.2.4 | Ensure SSH access is limited |  |  |
| 5.2.5 | Ensure SSH LogLevel is appropriate |  |  |
| 5.2.6 | Ensure SSH X11 forwarding is disabled |  |  |
| 5.2.7 | Ensure SSH MaxAuthTries is set to 4 or less |  |  |
| 5.2.8 | Ensure SSH IgnoreRhosts is enabled |  |  |
| 5.2.9 | Ensure SSH HostbasedAuthentication is disabled |  |  |
| 5.2.10 | Ensure SSH root login is disabled |  |  |
| 5.2.11 | Ensure SSH PermitEmptyPasswords is disabled |  |  |
| 5.2.12 | Ensure SSH PermitUserEnvironment is disabled |  |  |
| 5.2.13 | Ensure only strong Ciphers are used |  |  |
| 5.2.14 | Ensure only strong MAC algorithms are used |  |  |
| 5.2.15 | Ensure only strong Key Exchange algorithms are used |  |  |
| 5.2.16 | Ensure SSH Idle Timeout Interval is configured |  |  |
| 5.2.17 | Ensure SSH LoginGraceTime is set to one minute or less |  |  |
| 5.2.18 | Ensure SSH warning banner is configured |  |  |
| 5.2.19 | Ensure SSH PAM is enabled |  |  |
| 5.2.20 | Ensure SSH AllowTcpForwarding is disabled |  |  |
| 5.2.21 | Ensure SSH MaxStartups is configured |  |  |
| 5.2.22 | Ensure SSH MaxSessions is limited |  |  |
| 5.3.1 | Ensure password creation requirements are configured |  |  |
| 5.3.2 | Ensure lockout for failed password attempts is configured |  |  |
| 5.3.3 | Ensure password reuse is limited |  |  |
| 5.4.1.1 | Ensure password hashing algorithm is SHA-512 |  |  |
| 5.4.1.2 | Ensure password expiration is 365 days or less |  |  |



560 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 5.4.1.3 | Ensure minimum days between password changes is |  |  |
|  | configured |  |  |
| 5.4.1.4 | Ensure password expiration warning days is 7 or more |  |  |
| 5.4.1.5 | Ensure inactive password lock is 30 days or less |  |  |
| 5.4.1.6 | Ensure all users last password change date is in the past |  |  |
| 5.4.2 | Ensure system accounts are secured |  |  |
| 5.4.3 | Ensure default group for the root account is GID 0 |  |  |
| 5.4.4 | Ensure default user shell timeout is configured |  |  |
| 5.4.5 | Ensure default user umask is configured |  |  |
| 5.5 | Ensure root login is restricted to system console |  |  |
| 5.6 | Ensure access to the su command is restricted |  |  |
| 6.1.1 | Audit system file permissions |  |  |
| 6.1.2 | Ensure permissions on /etc/passwd are configured |  |  |
| 6.1.3 | Ensure permissions on /etc/shadow are configured |  |  |
| 6.1.4 | Ensure permissions on /etc/group are configured |  |  |
| 6.1.5 | Ensure permissions on /etc/passwd- are configured |  |  |
| 6.1.6 | Ensure permissions on /etc/shadow- are configured |  |  |
| 6.1.7 | Ensure permissions on /etc/group- are configured |  |  |
| 6.1.8 | Ensure no world writable files exist |  |  |
| 6.1.9 | Ensure no unowned files or directories exist |  |  |
| 6.1.10 | Ensure no ungrouped files or directories exist |  |  |
| 6.1.11 | Audit SUID executables |  |  |
| 6.1.12 | Audit SGID executables |  |  |
| 6.2.1 | Ensure accounts in /etc/passwd use shadowed passwords |  |  |
| 6.2.2 | Ensure /etc/shadow password fields are not empty |  |  |
| 6.2.3 | Ensure root is the only UID 0 account |  |  |
| 6.2.4 | Ensure root PATH Integrity |  |  |
| 6.2.5 | Ensure all users' home directories exist |  |  |
| 6.2.6 | Ensure users' home directories permissions are 750 or |  |  |
|  | more restrictive |  |  |
| 6.2.7 | Ensure users own their home directories |  |  |
| 6.2.8 | Ensure users' dot files are not group or world writable |  |  |
| 6.2.9 | Ensure no users have .forward files |  |  |
| 6.2.10 | Ensure no users have .netrc files |  |  |
| 6.2.11 | Ensure users' .netrc Files are not group or world accessible |  |  |
| 6.2.12 | Ensure no users have .rhosts files |  |  |
| 6.2.13 | Ensure all groups in /etc/passwd exist in /etc/group |  |  |
| 6.2.14 | Ensure no duplicate UIDs exist |  |  |
| 6.2.15 | Ensure no duplicate GIDs exist |  |  |
| 6.2.16 | Ensure no duplicate user names exist |  |  |
| 6.2.17 | Ensure no duplicate group names exist |  |  |
| 6.2.18 | Ensure shadow group is empty |  |  |



561 | P a g e



562 | P a g e

**Appendix: CIS Controls v8 IG 3 Mapped Recommendations**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Recommendation** | **Set** | |
|  |  | **Correctly** | |
|  |  | Yes | No |
| 1.1.1.1 | Ensure mounting of squashfs filesystems is disabled |  |  |
| 1.1.1.2 | Ensure mounting of udf filesystems is disabled |  |  |
| 1.1.1.3 | Ensure mounting of FAT filesystems is limited |  |  |
| 1.1.2 | Ensure /tmp is configured |  |  |
| 1.1.3 | Ensure noexec option set on /tmp partition |  |  |
| 1.1.4 | Ensure nodev option set on /tmp partition |  |  |
| 1.1.5 | Ensure nosuid option set on /tmp partition |  |  |
| 1.1.6 | Ensure /dev/shm is configured |  |  |
| 1.1.7 | Ensure noexec option set on /dev/shm partition |  |  |
| 1.1.8 | Ensure nodev option set on /dev/shm partition |  |  |
| 1.1.9 | Ensure nosuid option set on /dev/shm partition |  |  |
| 1.1.10 | Ensure separate partition exists for /var |  |  |
| 1.1.11 | Ensure separate partition exists for /var/tmp |  |  |
| 1.1.12 | Ensure noexec option set on /var/tmp partition |  |  |
| 1.1.13 | Ensure nodev option set on /var/tmp partition |  |  |
| 1.1.14 | Ensure nosuid option set on /var/tmp partition |  |  |
| 1.1.15 | Ensure separate partition exists for /var/log |  |  |
| 1.1.16 | Ensure separate partition exists for /var/log/audit |  |  |
| 1.1.17 | Ensure separate partition exists for /home |  |  |
| 1.1.18 | Ensure nodev option set on /home partition |  |  |
| 1.1.19 | Ensure noexec option set on removable media partitions |  |  |
| 1.1.20 | Ensure nodev option set on removable media partitions |  |  |
| 1.1.21 | Ensure nosuid option set on removable media partitions |  |  |
| 1.1.22 | Ensure sticky bit is set on all world-writable directories |  |  |
| 1.1.23 | Disable Automounting |  |  |
| 1.2.1 | Ensure GPG keys are configured |  |  |
| 1.2.2 | Ensure package manager repositories are configured |  |  |
| 1.2.3 | Ensure gpgcheck is globally activated |  |  |
| 1.3.1 | Ensure sudo is installed |  |  |
| 1.3.2 | Ensure sudo commands use pty |  |  |
| 1.3.3 | Ensure sudo log file exists |  |  |
| 1.4.1 | Ensure AIDE is installed |  |  |
| 1.4.2 | Ensure filesystem integrity is regularly checked |  |  |
| 1.5.1 | Ensure bootloader password is set |  |  |
| 1.5.2 | Ensure permissions on bootloader config are configured |  |  |
| 1.5.3 | Ensure authentication required for single user mode |  |  |
| 1.6.1 | Ensure core dumps are restricted |  |  |



563 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 1.6.2 | Ensure XD/NX support is enabled |  |  |
| 1.6.3 | Ensure address space layout randomization (ASLR) is |  |  |
|  | enabled |  |  |
| 1.6.4 | Ensure prelink is disabled |  |  |
| 1.7.1.1 | Ensure AppArmor is installed |  |  |
| 1.7.1.2 | Ensure AppArmor is enabled in the bootloader |  |  |
|  | configuration |  |  |
| 1.7.1.3 | Ensure all AppArmor Profiles are in enforce or complain |  |  |
|  | mode |  |  |
| 1.7.1.4 | Ensure all AppArmor Profiles are enforcing |  |  |
| 1.8.1.1 | Ensure message of the day is configured properly |  |  |
| 1.8.1.2 | Ensure local login warning banner is configured properly |  |  |
| 1.8.1.3 | Ensure remote login warning banner is configured properly |  |  |
| 1.8.1.4 | Ensure permissions on /etc/motd are configured |  |  |
| 1.8.1.5 | Ensure permissions on /etc/issue are configured |  |  |
| 1.8.1.6 | Ensure permissions on /etc/issue.net are configured |  |  |
| 1.9 | Ensure updates, patches, and additional security software |  |  |
|  | are installed |  |  |
| 1.10 | Ensure GDM is removed or login is configured |  |  |
| 2.1.1 | Ensure xinetd is not installed |  |  |
| 2.2.1.1 | Ensure time synchronization is in use |  |  |
| 2.2.1.2 | Ensure systemd-timesyncd is configured |  |  |
| 2.2.1.3 | Ensure chrony is configured |  |  |
| 2.2.2 | Ensure X11 Server components are not installed |  |  |
| 2.2.3 | Ensure Avahi Server is not installed |  |  |
| 2.2.4 | Ensure CUPS is not installed |  |  |
| 2.2.5 | Ensure DHCP Server is not installed |  |  |
| 2.2.6 | Ensure LDAP server is not installed |  |  |
| 2.2.7 | Ensure nfs-utils is not installed or the nfs-server service is |  |  |
|  | masked |  |  |
| 2.2.8 | Ensure rpcbind is not installed or the rpcbind services are |  |  |
|  | masked |  |  |
| 2.2.9 | Ensure DNS Server is not installed |  |  |
| 2.2.10 | Ensure FTP Server is not installed |  |  |
| 2.2.11 | Ensure HTTP server is not installed |  |  |
| 2.2.12 | Ensure IMAP and POP3 server is not installed |  |  |
| 2.2.13 | Ensure Samba is not installed |  |  |
| 2.2.14 | Ensure HTTP Proxy Server is not installed |  |  |
| 2.2.15 | Ensure net-snmp is not installed |  |  |
| 2.2.16 | Ensure mail transfer agent is configured for local-only mode |  |  |
| 2.2.17 | Ensure rsync is not installed or the rsyncd service is masked |  |  |
| 2.2.18 | Ensure NIS server is not installed |  |  |
| 2.2.19 | Ensure telnet-server is not installed |  |  |
| 2.3.1 | Ensure NIS Client is not installed |  |  |



564 | P a g e

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 2.3.2 | Ensure rsh client is not installed |  |  |  |  |
|  | 2.3.3 | Ensure talk client is not installed |  |  |  |  |
|  | 2.3.4 | Ensure telnet client is not installed |  |  |  |  |
|  | 2.3.5 | Ensure LDAP client is not installed |  |  |  |  |
|  | 2.4 | Ensure nonessential services are removed or masked |  |  |  |  |
|  | 3.1.1 | Disable IPv6 |  |  |  |  |
|  | 3.1.2 | Ensure wireless interfaces are disabled |  |  |  |  |
|  | 3.2.1 | Ensure IP forwarding is disabled |  |  |  |  |
|  | 3.2.2 | Ensure packet redirect sending is disabled |  |  |  |  |
|  | 3.3.1 | Ensure source routed packets are not accepted |  |  |  |  |
|  | 3.3.2 | Ensure ICMP redirects are not accepted |  |  |  |  |
|  | 3.3.3 | Ensure secure ICMP redirects are not accepted |  |  |  |  |
|  | 3.3.4 | Ensure suspicious packets are logged |  |  |  |  |
|  | 3.3.5 | Ensure broadcast ICMP requests are ignored |  |  |  |  |
|  | 3.3.6 | Ensure bogus ICMP responses are ignored |  |  |  |  |
|  | 3.3.7 | Ensure Reverse Path Filtering is enabled |  |  |  |  |
|  | 3.3.8 | Ensure TCP SYN Cookies is enabled |  |  |  |  |
|  | 3.3.9 | Ensure IPv6 router advertisements are not accepted |  |  |  |  |
|  | 3.4.1 | Ensure DCCP is disabled |  |  |  |  |
|  | 3.4.2 | Ensure SCTP is disabled |  |  |  |  |
|  | 3.5.1.1 | Ensure FirewallD is installed |  |  |  |  |
|  | 3.5.1.2 | Ensure nftables is not installed or stopped and masked |  |  |  |  |
|  | 3.5.1.3 | Ensure firewalld service is enabled and running |  |  |  |  |
|  | 3.5.1.4 | Ensure default zone is set |  |  |  |  |
|  | 3.5.1.5 | Ensure network interfaces are assigned to appropriate zone |  |  |  |  |
|  | 3.5.1.6 | Ensure unnecessary services and ports are not accepted |  |  |  |  |
|  | 3.5.2.1 | Ensure nftables is installed |  |  |  |  |
|  | 3.5.2.2 | Ensure firewalld is not installed or stopped and masked |  |  |  |  |
|  | 3.5.2.3 | Ensure iptables are flushed |  |  |  |  |
|  | 3.5.2.4 | Ensure a table exists |  |  |  |  |
|  | 3.5.2.5 | Ensure base chains exist |  |  |  |  |
|  | 3.5.2.6 | Ensure loopback traffic is configured |  |  |  |  |
|  | 3.5.2.7 | Ensure outbound and established connections are |  |  |  |  |
|  |  | configured |  |  |  |  |
|  | 3.5.2.8 | Ensure default deny firewall policy |  |  |  |  |
|  | 3.5.2.9 | Ensure nftables service is enabled |  |  |  |  |
|  | 3.5.2.10 | Ensure nftables rules are permanent |  |  |  |  |
|  | 3.5.3.1.1 | Ensure iptables package is installed |  |  |  |  |
|  | 3.5.3.1.2 | Ensure nftables is not installed |  |  |  |  |
|  | 3.5.3.1.3 | Ensure firewalld is not installed or stopped and masked |  |  |  |  |
|  | 3.5.3.2.1 | Ensure default deny firewall policy |  |  |  |  |
|  | 3.5.3.2.2 | Ensure loopback traffic is configured |  |  |  |  |
|  | 3.5.3.2.3 | Ensure outbound and established connections are |  |  |  |  |
|  |  | configured |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  | 565 | P a g e | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 3.5.3.2.4 | Ensure firewall rules exist for all open ports |  |  |  |  |
|  | 3.5.3.3.1 | Ensure IPv6 default deny firewall policy |  |  |  |  |
|  | 3.5.3.3.2 | Ensure IPv6 loopback traffic is configured |  |  |  |  |
|  | 3.5.3.3.3 | Ensure IPv6 outbound and established connections are |  |  |  |  |
|  |  | configured |  |  |  |  |
|  | 3.5.3.3.4 | Ensure IPv6 firewall rules exist for all open ports |  |  |  |  |
|  | 4.1.1.1 | Ensure auditd is installed |  |  |  |  |
|  | 4.1.1.2 | Ensure auditd service is enabled and running |  |  |  |  |
|  | 4.1.1.3 | Ensure auditing for processes that start prior to auditd is |  |  |  |  |
|  |  | enabled |  |  |  |  |
|  | 4.1.2.1 | Ensure audit log storage size is configured |  |  |  |  |
|  | 4.1.2.2 | Ensure audit logs are not automatically deleted |  |  |  |  |
|  | 4.1.2.3 | Ensure system is disabled when audit logs are full |  |  |  |  |
|  | 4.1.2.4 | Ensure audit\_backlog\_limit is sufficient |  |  |  |  |
|  | 4.1.3 | Ensure events that modify date and time information are |  |  |  |  |
|  |  | collected |  |  |  |  |
|  | 4.1.4 | Ensure events that modify user/group information are |  |  |  |  |
|  |  | collected |  |  |  |  |
|  | 4.1.5 | Ensure events that modify the system's network |  |  |  |  |
|  |  | environment are collected |  |  |  |  |
|  | 4.1.6 | Ensure events that modify the system's Mandatory Access |  |  |  |  |
|  |  | Controls are collected |  |  |  |  |
|  | 4.1.7 | Ensure login and logout events are collected |  |  |  |  |
|  | 4.1.8 | Ensure session initiation information is collected |  |  |  |  |
|  | 4.1.9 | Ensure discretionary access control permission |  |  |  |  |
|  |  | modification events are collected |  |  |  |  |
|  | 4.1.10 | Ensure unsuccessful unauthorized file access attempts are |  |  |  |  |
|  |  | collected |  |  |  |  |
|  | 4.1.11 | Ensure use of privileged commands is collected |  |  |  |  |
|  | 4.1.12 | Ensure successful file system mounts are collected |  |  |  |  |
|  | 4.1.13 | Ensure file deletion events by users are collected |  |  |  |  |
|  | 4.1.14 | Ensure changes to system administration scope (sudoers) is |  |  |  |  |
|  |  | collected |  |  |  |  |
|  | 4.1.15 | Ensure system administrator actions (sudolog) are collected |  |  |  |  |
|  | 4.1.16 | Ensure kernel module loading and unloading is collected |  |  |  |  |
|  | 4.1.17 | Ensure the audit configuration is immutable |  |  |  |  |
|  | 4.2.1.1 | Ensure rsyslog is installed |  |  |  |  |
|  | 4.2.1.2 | Ensure rsyslog Service is enabled and running |  |  |  |  |
|  | 4.2.1.3 | Ensure rsyslog default file permissions configured |  |  |  |  |
|  | 4.2.1.4 | Ensure logging is configured |  |  |  |  |
|  | 4.2.1.5 | Ensure rsyslog is configured to send logs to a remote log |  |  |  |  |
|  |  | host |  |  |  |  |
|  | 4.2.1.6 | Ensure remote rsyslog messages are only accepted on |  |  |  |  |
|  |  | designated log hosts. |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  | 566 | P a g e | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 4.2.2.1 | Ensure journald is configured to send logs to rsyslog |  |  |
| 4.2.2.2 | Ensure journald is configured to compress large log files |  |  |
| 4.2.2.3 | Ensure journald is configured to write logfiles to persistent |  |  |
|  | disk |  |  |
| 4.2.3 | Ensure permissions on all logfiles are configured |  |  |
| 4.2.4 | Ensure logrotate is configured |  |  |
| 5.1.1 | Ensure cron daemon is enabled and running |  |  |
| 5.1.2 | Ensure permissions on /etc/crontab are configured |  |  |
| 5.1.3 | Ensure permissions on /etc/cron.hourly are configured |  |  |
| 5.1.4 | Ensure permissions on /etc/cron.daily are configured |  |  |
| 5.1.5 | Ensure permissions on /etc/cron.weekly are configured |  |  |
| 5.1.6 | Ensure permissions on /etc/cron.monthly are configured |  |  |
| 5.1.7 | Ensure permissions on /etc/cron.d are configured |  |  |
| 5.1.8 | Ensure cron is restricted to authorized users |  |  |
| 5.1.9 | Ensure at is restricted to authorized users |  |  |
| 5.2.1 | Ensure permissions on /etc/ssh/sshd\_config are configured |  |  |
| 5.2.2 | Ensure permissions on SSH private host key files are |  |  |
|  | configured |  |  |
| 5.2.3 | Ensure permissions on SSH public host key files are |  |  |
|  | configured |  |  |
| 5.2.4 | Ensure SSH access is limited |  |  |
| 5.2.5 | Ensure SSH LogLevel is appropriate |  |  |
| 5.2.6 | Ensure SSH X11 forwarding is disabled |  |  |
| 5.2.7 | Ensure SSH MaxAuthTries is set to 4 or less |  |  |
| 5.2.8 | Ensure SSH IgnoreRhosts is enabled |  |  |
| 5.2.9 | Ensure SSH HostbasedAuthentication is disabled |  |  |
| 5.2.10 | Ensure SSH root login is disabled |  |  |
| 5.2.11 | Ensure SSH PermitEmptyPasswords is disabled |  |  |
| 5.2.12 | Ensure SSH PermitUserEnvironment is disabled |  |  |
| 5.2.13 | Ensure only strong Ciphers are used |  |  |
| 5.2.14 | Ensure only strong MAC algorithms are used |  |  |
| 5.2.15 | Ensure only strong Key Exchange algorithms are used |  |  |
| 5.2.16 | Ensure SSH Idle Timeout Interval is configured |  |  |
| 5.2.17 | Ensure SSH LoginGraceTime is set to one minute or less |  |  |
| 5.2.18 | Ensure SSH warning banner is configured |  |  |
| 5.2.19 | Ensure SSH PAM is enabled |  |  |
| 5.2.20 | Ensure SSH AllowTcpForwarding is disabled |  |  |
| 5.2.21 | Ensure SSH MaxStartups is configured |  |  |
| 5.2.22 | Ensure SSH MaxSessions is limited |  |  |
| 5.3.1 | Ensure password creation requirements are configured |  |  |
| 5.3.2 | Ensure lockout for failed password attempts is configured |  |  |
| 5.3.3 | Ensure password reuse is limited |  |  |
| 5.4.1.1 | Ensure password hashing algorithm is SHA-512 |  |  |
| 5.4.1.2 | Ensure password expiration is 365 days or less |  |  |



567 | P a g e

|  |  |  |  |
| --- | --- | --- | --- |
| 5.4.1.3 | Ensure minimum days between password changes is |  |  |
|  | configured |  |  |
| 5.4.1.4 | Ensure password expiration warning days is 7 or more |  |  |
| 5.4.1.5 | Ensure inactive password lock is 30 days or less |  |  |
| 5.4.1.6 | Ensure all users last password change date is in the past |  |  |
| 5.4.2 | Ensure system accounts are secured |  |  |
| 5.4.3 | Ensure default group for the root account is GID 0 |  |  |
| 5.4.4 | Ensure default user shell timeout is configured |  |  |
| 5.4.5 | Ensure default user umask is configured |  |  |
| 5.5 | Ensure root login is restricted to system console |  |  |
| 5.6 | Ensure access to the su command is restricted |  |  |
| 6.1.1 | Audit system file permissions |  |  |
| 6.1.2 | Ensure permissions on /etc/passwd are configured |  |  |
| 6.1.3 | Ensure permissions on /etc/shadow are configured |  |  |
| 6.1.4 | Ensure permissions on /etc/group are configured |  |  |
| 6.1.5 | Ensure permissions on /etc/passwd- are configured |  |  |
| 6.1.6 | Ensure permissions on /etc/shadow- are configured |  |  |
| 6.1.7 | Ensure permissions on /etc/group- are configured |  |  |
| 6.1.8 | Ensure no world writable files exist |  |  |
| 6.1.9 | Ensure no unowned files or directories exist |  |  |
| 6.1.10 | Ensure no ungrouped files or directories exist |  |  |
| 6.1.11 | Audit SUID executables |  |  |
| 6.1.12 | Audit SGID executables |  |  |
| 6.2.1 | Ensure accounts in /etc/passwd use shadowed passwords |  |  |
| 6.2.2 | Ensure /etc/shadow password fields are not empty |  |  |
| 6.2.3 | Ensure root is the only UID 0 account |  |  |
| 6.2.4 | Ensure root PATH Integrity |  |  |
| 6.2.5 | Ensure all users' home directories exist |  |  |
| 6.2.6 | Ensure users' home directories permissions are 750 or |  |  |
|  | more restrictive |  |  |
| 6.2.7 | Ensure users own their home directories |  |  |
| 6.2.8 | Ensure users' dot files are not group or world writable |  |  |
| 6.2.9 | Ensure no users have .forward files |  |  |
| 6.2.10 | Ensure no users have .netrc files |  |  |
| 6.2.11 | Ensure users' .netrc Files are not group or world accessible |  |  |
| 6.2.12 | Ensure no users have .rhosts files |  |  |
| 6.2.13 | Ensure all groups in /etc/passwd exist in /etc/group |  |  |
| 6.2.14 | Ensure no duplicate UIDs exist |  |  |
| 6.2.15 | Ensure no duplicate GIDs exist |  |  |
| 6.2.16 | Ensure no duplicate user names exist |  |  |
| 6.2.17 | Ensure no duplicate group names exist |  |  |
| 6.2.18 | Ensure shadow group is empty |  |  |



568 | P a g e



569 | P a g e

**Appendix: Change History**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Date | Version | Changes for this version |
|  | Jan 24, 2022 | 1.1.1 | 3.5.3.2.4 - UPDATE - Artifact - Updated |
|  |  |  | artifact to use SCE scripts. This better |
|  |  |  | aligns with other benchmarks |
|  |  |  | validating iptables rules on open |
|  |  |  | ports. |
|  | Jan 24, 2022 | 1.1.1 | 6.2.5 - UPDATE - Artifact - Changed |
|  |  |  | automation to align with upstream |
|  |  |  | Fedora method using SCE script |
|  | Jan 24, 2022 | 1.1.1 | 6.2.6 - UPDATE - Artifact - Changed |
|  |  |  | automation to align with upstream |
|  |  |  | Fedora method using SCE script |
|  | Jan 24, 2022 | 1.1.1 | 6.2.7 - - UPDATE - Artifact - Changed |
|  |  |  | automation to align with upstream |
|  |  |  | Fedora method using SCE script |
|  | Jan 24, 2022 | 1.1.1 | 6.2.8 - UPDATE - Artifact - Changed |
|  |  |  | automation to align with upstream |
|  |  |  | Fedora method using SCE script |
|  | Jan 24, 2022 | 1.1.1 | 6.2.9 - UPDATE - Artifact - Changed |
|  |  |  | automation to align with upstream |
|  |  |  | Fedora method using SCE script |
|  | Jan 24, 2022 | 1.1.1 | 6.2.10 - UPDATE - Artifact - Changed |
|  |  |  | automation to align with upstream |
|  |  |  | Fedora method using SCE script |
|  | Jan 24, 2022 | 1.1.1 | 6.2.11 - UPDATE - Artifact - Changed |
|  |  |  | automation to align with upstream |
|  |  |  | Fedora method using SCE script |
|  | Jan 24, 2022 | 1.1.1 | 6.2.12 - UPDATE - Artifact - Changed |
|  |  |  | automation to align with upstream |
|  |  |  | Fedora method using SCE script |
|  | Aug 24, 2021 | 1.1.0 | 4.1.3 - UPDATE: Audit - Issue with |
|  |  |  | 'Verify Output of both matches' in the |
|  |  |  | '64 bit system' direction. (Ticket |
|  |  |  | 11976) |
|  | Aug 24, 2021 | 1.1.0 | 4.1.5 - UPDATE: Audit, Remediation - |
|  |  |  | 'Verify Output' for 64bit system |
|  |  |  | change - system-local (Ticket 13525) |
|  | Aug 24, 2021 | 1.1.0 | 1.1.2 - UPDATE: Remediation - Typo |
|  |  |  | in Remediation 'tmp.mpunt' (Ticket |
|  |  |  | 13488) |
|  | Aug 24, 2021 | 1.1.0 | 1.1.2 - UPDATE: Remediation - Typo |
|  |  |  | in Example tmp.mount file (Ticket |
|  |  |  | 13249) |



570 | P a g e

|  |  |  |
| --- | --- | --- |
| Aug 24, 2021 | 1.1.0 | 1.1.3 - UPDATE: Additional Info - |
|  |  | incorrect path to systemd tmp.mount |
|  |  | file (Ticket 12912) |
| Aug 24, 2021 | 1.1.0 | 1.1.4 - UPDATE: Additional Info - |
|  |  | incorrect path to systemd tmp.mount |
|  |  | file (Ticket 13543) |
| Aug 24, 2021 | 1.1.0 | 1.1.5 - UPDATE: Additional Info - |
|  |  | incorrect path to systemd tmp.mount |
|  |  | file (Ticket 13544) |
| Aug 24, 2021 | 1.1.0 | 4.1.4 - UPDATE: Audit, Remediation, |
|  |  | Artifacts - gshadow obsolete reference |
|  |  | (Ticket 12153) |
| Aug 24, 2021 | 1.1.0 | 1.4.2 - UPDATE: Audit - Typo in Audit |
|  |  | procedure (Ticket 13250) |
| Aug 24, 2021 | 1.1.0 | 4.1.2.4 - UPDATE: Audit - Double |
|  |  | occurrence in Audit Procedure (Ticket |
|  |  | 13252) |
| Aug 24, 2021 | 1.1.0 | 1.4.1 - UPDATE: Reference - Reference |
|  |  | error to Aide manual (Ticket 12102) |
| Aug 24, 2021 | 1.1.0 | 4.1.6 - UPDATE: Audit - 'Verify Output' |
|  |  | for 64bit system change - MAC-policy |
|  |  | (Ticket 13526) |
| Aug 24, 2021 | 1.1.0 | 4.1.7 - UPDATE: Audit - 'Verify Output' |
|  |  | for 64bit system change - logins |
|  |  | (Ticket 13527) |
| Aug 24, 2021 | 1.1.0 | 4.1.8 - UPDATE: Audit - 'Verify Output' |
|  |  | for 64bit system change - sessions |
|  |  | (Ticket 13528) |
| Aug 24, 2021 | 1.1.0 | 4.1.9 - UPDATE: Audit - 'Verify Output' |
|  |  | for 64bit system change - perm-mod |
|  |  | (Ticket 13529) |
| Aug 24, 2021 | 1.1.0 | 4.1.10 - UPDATE: Audit - 'Verify |
|  |  | Output' for 64bit system change - |
|  |  | access (Ticket 13530) |
| Aug 24, 2021 | 1.1.0 | 4.1.12 - UPDATE: Audit, Remediation - |
|  |  | 'Verify Output' for 64bit system |
|  |  | change - mounts (Ticket 13531) |
| Aug 24, 2021 | 1.1.0 | 4.1.13 - UPDATE: Audit - 'Verify |
|  |  | Output' for 64bit system change - |
|  |  | deletion (Ticket 13532) |
| Aug 24, 2021 | 1.1.0 | 4.1.14 - UPDATE: Audit - 'Verify |
|  |  | Output' for 64bit system change - |
|  |  | scope (Ticket 13533) |
| Aug 24, 2021 | 1.1.0 | 4.1.16 - UPDATE: Audit - 'Verify |
|  |  | Output' for 64bit system change - |
|  |  | modules (Ticket 13534) |



571 | P a g e

|  |  |  |
| --- | --- | --- |
| Aug 25, 2021 | 1.1.0 | 4.1.5 - UPDATE: Audit, Remediation, |
|  |  | Artifact - Consider update for issue- |
|  |  | generator (Ticket 13553) |
| Aug 31, 2021 | 1.1.0 | 3.5.2.1 - UPDATE: Artifact - Update to |
|  |  | use new SUSE specific nftables script |
|  |  | (Ticket 13652) |
| Aug 31, 2021 | 1.1.0 | 3.5.2.2 - UPDATE: Artifact - Update to |
|  |  | use new SUSE specific nftables script |
|  |  | (Ticket 13653) |
| Aug 31, 2021 | 1.1.0 | 3.5.2.4 - UPDATE: Artifact - Update to |
|  |  | use new SUSE specific nftables script |
|  |  | (Ticket 13654) |
| Aug 31, 2021 | 1.1.0 | 3.5.2.5 - UPDATE: Artifact - Update to |
|  |  | use new SUSE specific nftables script |
|  |  | (Ticket 13655) |
| Aug 31, 2021 | 1.1.0 | 3.5.2.6 - UPDATE: Artifact - Update to |
|  |  | use new SUSE specific nftables script |
|  |  | (Ticket 13656) |
| Aug 31, 2021 | 1.1.0 | 3.5.2.8 - UPDATE: Artifact - Update to |
|  |  | use new SUSE specific nftables script |
|  |  | (Ticket 13657) |
| Aug 31, 2021 | 1.1.0 | 3.5.2.9 - UPDATE: Artifact - Update to |
|  |  | use new SUSE specific nftables script |
|  |  | (Ticket 13658) |
| Aug 31, 2021 | 1.1.0 | 3.5.2.10 - UPDATE: Artifiact - Update |
|  |  | to use new SUSE specific nftables |
|  |  | script (Ticket 13659) |
| Aug 31, 2021 | 1.1.0 | 1.4.2 - UPDATE: Artifact - Root |
|  |  | crontab path incorrect for SLES 15 |
|  |  | SP3 (Ticket 13612) |
| Aug 31, 2021 | 1.1.0 | 1.8.1.6 - UPDATE: Artifact - Issue.net |
|  |  | does not exist on SLES 15 SP3 (Ticket |
|  |  | 13613) |
| Sep 1, 2021 | 1.1.0 | 5.3.2 - UPDATE: Audit, Remediation, |
|  |  | Artifact - SUSE needs the unlock set in |
|  |  | /etc/pam.d/login file (Ticket 13665) |
| Sep 1, 2021 | 1.1.0 | Draft published for consensus review |
| Sep 21, 2021 | 1.1.0 | Final version published |



572 | P a g e