Security Configuration Assessment Report for controlplane

Target IP Address: 10.244.0.0

CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0

Level 1 - Server
Monday, August 28 2023 00:32:16
Assessment Duration: 1 minute, 24 seconds

Summary

Description	Tests					Scoring		
	Pass	Fail	Error	Unkn.	Man.	Score	Max	Percent
1 Initial Setup	**38**	**17**	**0**	**0**	**3**	**38.0**	**55.0**	**69%**
1.1 Filesystem Configuration	20	7	0	0	0	20.0	27.0	74%
1.1.1 Disable unused filesystems	0	5	0	0	0	0.0	5.0	0%
1.1.2 Configure /tmp	3	1	0	0	0	3.0	4.0	75%
1.1.3 Configure /var	2	0	0	0	0	2.0	2.0	100%
1.1.4 Configure /var/tmp	3	0	0	0	0	3.0	3.0	100%
1.1.5 Configure /var/log	3	0	0	0	0	3.0	3.0	100%
1.1.6 Configure /var/log/audit	3	0	0	0	0	3.0	3.0	100%
1.1.7 Configure /home	2	0	0	0	0	2.0	2.0	100%
1.1.8 Configure /dev/shm	3	0	0	0	0	3.0	3.0	100%
1.2 Filesystem Integrity Checking	0	2	0	0	0	0.0	2.0	0%
1.3 Configure Software and Patch Management	0	0	0	0	3	0.0	0.0	0%
1.4 Secure Boot Settings	1	2	0	0	0	1.0	3.0	33%
1.5 Additional Process Hardening	3	2	0	0	0	3.0	5.0	60%
1.6 Mandatory Access Control	0	3	0	0	0	0.0	3.0	0%
1.6.1 Configure AppArmor	0	3	0	0	0	0.0	3.0	0%
1.7 Command Line Warning Banners	5	1	0	0	0	5.0	6.0	83%
1.8 GNOME Display Manager	9	0	0	0	0	9.0	9.0	100%
2 Services	**26**	**3**	**0**	**0**	**4**	**26.0**	**29.0**	**90%**
2.1 Configure Time Synchronization	6	1	0	0	3	6.0	7.0	86%
2.1.1 Ensure time synchronization is in use	1	0	0	0	0	1.0	1.0	100%
2.1.2 Configure chrony	2	0	0	0	1	2.0	2.0	100%
2.1.3 Configure systemd-timesyncd	0	1	0	0	1	0.0	1.0	0%
2.1.4 Configure ntp	3	0	0	0	1	3.0	3.0	100%
2.2 Special Purpose Services	15	1	0	0	0	15.0	16.0	94%
2.3 Service Clients	5	1	0	0	0	5.0	6.0	83%
3 Network Configuration	**7**	**29**	**0**	**0**	**6**	**7.0**	**36.0**	**19%**
3.1 Disable unused network protocols and devices	2	0	0	0	1	2.0	2.0	100%
3.2 Network Parameters (Host Only)	0	2	0	0	0	0.0	2.0	0%
3.3 Network Parameters (Host and Router)	0	9	0	0	0	0.0	9.0	0%
3.4 Firewall Configuration	5	18	0	0	5	5.0	23.0	22%
3.4.1 Configure UncomplicatedFirewall	1	5	0	0	1	1.0	6.0	17%
3.4.2 Configure nftables	1	7	0	0	2	1.0	8.0	12%
3.4.3 Configure iptables	3	6	0	0	2	3.0	9.0	33%
3.4.3.1 Configure iptables software	2	1	0	0	0	2.0	3.0	67%
3.4.3.2 Configure IPv4 iptables	0	3	0	0	1	0.0	3.0	0%
3.4.3.3 Configure IPv6 ip6tables	1	2	0	0	1	1.0	3.0	33%
4 Access, Authentication and Authorization	**25**	**26**	**0**	**0**	**1**	**25.0**	**51.0**	**49%**
4.1 Configure time-based job schedulers	3	6	0	0	0	3.0	9.0	33%
4.2 Configure SSH Server	14	6	0	0	0	14.0	20.0	70%
4.3 Configure privilege escalation	3	3	0	0	0	3.0	6.0	50%
4.4 Configure PAM	1	3	0	0	1	1.0	4.0	25%
4.5 User Accounts and Environment	4	8	0	0	0	4.0	12.0	33%
4.5.1 Set Shadow Password Suite Parameters	2	5	0	0	0	2.0	7.0	29%
5 Logging and Auditing	**7**	**4**	**0**	**0**	**8**	**7.0**	**11.0**	**64%**
5.1 Configure Logging	7	3	0	0	8	7.0	10.0	70%
5.1.1 Configure journald	3	2	0	0	5	3.0	5.0	60%
5.1.1.1 Ensure journald is configured to send logs to a remote log host	2	0	0	0	2	2.0	2.0	100%
5.1.2 Configure rsyslog	4	0	0	0	3	4.0	4.0	100%
5.2 Configure System Accounting (auditd)	0	1	0	0	0	0.0	1.0	0%
5.2.1 Ensure auditing is enabled	0	0	0	0	0	0.0	0.0	0%
5.2.2 Configure Data Retention	0	0	0	0	0	0.0	0.0	0%
5.2.3 Configure auditd rules	0	0	0	0	0	0.0	0.0	0%
5.2.4 Configure auditd file access	0	1	0	0	0	0.0	1.0	0%
6 System Maintenance	**19**	**5**	**0**	**0**	**1**	**19.0**	**24.0**	**79%**
6.1 System File Permissions	9	3	0	0	1	9.0	12.0	75%
6.2 Local User and Group Settings	10	2	0	0	0	10.0	12.0	83%
Total	**122**	**84**	**0**	**0**	**23**	**122.0**	**206.0**	**59%**

Note: Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.

Profiles

This benchmark contains 4 profiles.The **Level 1 - Server** profile was used for this assessment.

Title	Description
Level 1 - Server	Items in this profile intend to: • be practical and prudent; • provide a clear security benefit; and • not inhibit the utility of the technology beyond acceptable means. This profile is intended for servers. Show Profile XML
Level 2 - Server	This profile extends the "Level 1 - Server" profile. Items in this profile exhibit one or more of the following characteristics: • are intended for environments or use cases where security is paramount. • acts as defense in depth measure. • may negatively inhibit the utility or performance of the technology. This profile is intended for servers. Show Profile XML
Level 1 - Workstation	Items in this profile intend to: • be practical and prudent; • provide a clear security benefit; and • not inhibit the utility of the technology beyond acceptable means. This profile is intended for workstations. Show Profile XML
Level 2 - Workstation	This profile extends the "Level 1 - Workstation" profile. Items in this profile exhibit one or more of the following characteristics: • are intended for environments or use cases where security is paramount. • acts as defense in depth measure. • may negatively inhibit the utility or performance of the technology. This profile is intended for workstations. Show Profile XML

⇧

Assessment Results

☐ Display Only Essential Hygiene (CIS Critical Security Controls V8- IG-1) ☐ Display Only Failures

More

w	Benchmark Item	Result
1 Initial Setup		
1.1 Filesystem Configuration		
1.1.1 Disable unused filesystems		
1.0	1.1.1.1 Ensure mounting of cramfs filesystems is disabled	Fail
1.0	1.1.1.2 Ensure mounting of freevxfs filesystems is disabled	Fail
1.0	1.1.1.3 Ensure mounting of jffs2 filesystems is disabled	Fail
1.0	1.1.1.4 Ensure mounting of hfs filesystems is disabled	Fail
1.0	1.1.1.5 Ensure mounting of hfsplus filesystems is disabled	Fail
1.1.2 Configure /tmp		
1.0	1.1.2.1 Ensure /tmp is a separate partition	Fail
1.0	1.1.2.2 Ensure nodev option set on /tmp partition	Pass
1.0	1.1.2.3 Ensure noexec option set on /tmp partition	Pass
1.0	1.1.2.4 Ensure nosuid option set on /tmp partition	Pass
1.1.3 Configure /var		
1.0	1.1.3.2 Ensure nodev option set on /var partition	Pass
1.0	1.1.3.3 Ensure nosuid option set on /var partition	Pass
1.1.4 Configure /var/tmp		
1.0	1.1.4.2 Ensure nodev option set on /var/tmp partition	Pass
1.0	1.1.4.3 Ensure noexec option set on /var/tmp partition	Pass
1.0	1.1.4.4 Ensure nosuid option set on /var/tmp partition	Pass
1.1.5 Configure /var/log		
1.0	1.1.5.2 Ensure nodev option set on /var/log partition	Pass
1.0	1.1.5.3 Ensure noexec option set on /var/log partition	Pass

	Benchmark Item	Result
1.0	1.1.5.4 Ensure nosuid option set on /var/log partition	Pass
	1.1.6 Configure /var/log/audit	
1.0	1.1.6.2 Ensure nodev option set on /var/log/audit partition	Pass
1.0	1.1.6.3 Ensure noexec option set on /var/log/audit partition	Pass
1.0	1.1.6.4 Ensure nosuid option set on /var/log/audit partition	Pass
	1.1.7 Configure /home	
1.0	1.1.7.2 Ensure nodev option set on /home partition	Pass
1.0	1.1.7.3 Ensure nosuid option set on /home partition	Pass
	1.1.8 Configure /dev/shm	
1.0	1.1.8.1 Ensure nodev option set on /dev/shm partition	Pass
1.0	1.1.8.2 Ensure noexec option set on /dev/shm partition	Pass
1.0	1.1.8.3 Ensure nosuid option set on /dev/shm partition	Pass
1.0	1.1.9 Disable Automounting	Pass
1.0	1.1.10 Disable USB Storage	Fail
	1.2 Filesystem Integrity Checking	
1.0	1.2.1 Ensure AIDE is installed	Fail
1.0	1.2.2 Ensure filesystem integrity is regularly checked	Fail
	1.3 Configure Software and Patch Management	
	1.3.1 Ensure updates, patches, and additional security software are installed	Manual
	1.3.2 Ensure package manager repositories are configured	Manual
	1.3.3 Ensure GPG keys are configured	Manual
	1.4 Secure Boot Settings	
1.0	1.4.1 Ensure bootloader password is set	Fail
1.0	1.4.2 Ensure permissions on bootloader config are configured	Fail
1.0	1.4.3 Ensure authentication required for single user mode	Pass
	1.5 Additional Process Hardening	
1.0	1.5.1 Ensure prelink is not installed	Pass
1.0	1.5.2 Ensure address space layout randomization (ASLR) is enabled	Fail
1.0	1.5.3 Ensure ptrace_scope is restricted	Pass
1.0	1.5.4 Ensure Automatic Error Reporting is not enabled	Pass
1.0	1.5.5 Ensure core dumps are restricted	Fail
	1.6 Mandatory Access Control	
	1.6.1 Configure AppArmor	
1.0	1.6.1.1 Ensure AppArmor is installed	Fail
1.0	1.6.1.2 Ensure AppArmor is enabled in the bootloader configuration	Fail
1.0	1.6.1.3 Ensure all AppArmor Profiles are in enforce or complain mode	Fail
	1.7 Command Line Warning Banners	
1.0	1.7.1 Ensure message of the day is configured properly	Pass
1.0	1.7.2 Ensure local login warning banner is configured properly	Pass
1.0	1.7.3 Ensure remote login warning banner is configured properly	Fail
1.0	1.7.4 Ensure permissions on /etc/motd are configured	Pass
1.0	1.7.5 Ensure permissions on /etc/issue are configured	Pass
1.0	1.7.6 Ensure permissions on /etc/issue.net are configured	Pass
	1.8 GNOME Display Manager	
1.0	1.8.2 Ensure GDM login banner is configured	Pass
1.0	1.8.3 Ensure GDM disable-user-list option is enabled	Pass
1.0	1.8.4 Ensure GDM screen locks when the user is idle	Pass
1.0	1.8.5 Ensure GDM screen locks cannot be overridden	Pass
1.0	1.8.6 Ensure GDM automatic mounting of removable media is disabled	Pass
1.0	1.8.7 Ensure GDM disabling automatic mounting of removable media is not overridden	Pass
1.0	1.8.8 Ensure GDM autorun-never is enabled	Pass
1.0	1.8.9 Ensure GDM autorun-never is not overridden	Pass
1.0	1.8.10 Ensure XDCMP is not enabled	Pass
	2 Services	
	2.1 Configure Time Synchronization	
	2.1.1 Ensure time synchronization is in use	
1.0	2.1.1.1 Ensure a single time synchronization daemon is in use	Pass
	2.1.2 Configure chrony	
	2.1.2.1 Ensure chrony is configured with authorized timeserver	Manual

w	Benchmark Item	Result
1.0	2.1.2.2 Ensure chrony is running as user _chrony	Pass
1.0	2.1.2.3 Ensure chrony is enabled and running	Pass
	2.1.3 Configure systemd-timesyncd	
1.0	2.1.3.1 Ensure systemd-timesyncd configured with authorized timeserver	Fail
	2.1.3.2 Ensure systemd-timesyncd is enabled and running	Manual
	2.1.4 Configure ntp	
1.0	2.1.4.1 Ensure ntp access control is configured	Pass
	2.1.4.2 Ensure ntp is configured with authorized timeserver	Manual
1.0	2.1.4.3 Ensure ntp is running as user ntp	Pass
1.0	2.1.4.4 Ensure ntp is enabled and running	Pass
	2.2 Special Purpose Services	
1.0	2.2.2 Ensure Avahi Server is not installed	Pass
1.0	2.2.3 Ensure CUPS is not installed	Pass
1.0	2.2.4 Ensure DHCP Server is not installed	Pass
1.0	2.2.5 Ensure LDAP server is not installed	Pass
1.0	2.2.6 Ensure NFS is not installed	Pass
1.0	2.2.7 Ensure DNS Server is not installed	Pass
1.0	2.2.8 Ensure FTP Server is not installed	Pass
1.0	2.2.9 Ensure HTTP server is not installed	Fail
1.0	2.2.10 Ensure IMAP and POP3 server are not installed	Pass
1.0	2.2.11 Ensure Samba is not installed	Pass
1.0	2.2.12 Ensure HTTP Proxy Server is not installed	Pass
1.0	2.2.13 Ensure SNMP Server is not installed	Pass
1.0	2.2.14 Ensure NIS Server is not installed	Pass
1.0	2.2.15 Ensure dnsmasq is not installed	Pass
1.0	2.2.16 Ensure mail transfer agent is configured for local-only mode	Pass
1.0	2.2.17 Ensure rsync service is either not installed or is masked	Pass
	2.3 Service Clients	
1.0	2.3.1 Ensure NIS Client is not installed	Pass
1.0	2.3.2 Ensure rsh client is not installed	Pass
1.0	2.3.3 Ensure talk client is not installed	Pass
1.0	2.3.4 Ensure telnet client is not installed	Fail
1.0	2.3.5 Ensure LDAP client is not installed	Pass
1.0	2.3.6 Ensure RPC is not installed	Pass
	2.4 Ensure nonessential services are removed or masked	Manual
	3 Network Configuration	
	3.1 Disable unused network protocols and devices	
	3.1.1 Ensure IPv6 status is identified	Manual
1.0	3.1.2 Ensure wireless interfaces are disabled	Pass
1.0	3.1.3 Ensure bluetooth is disabled	Pass
	3.2 Network Parameters (Host Only)	
1.0	3.2.1 Ensure packet redirect sending is disabled	Fail
1.0	3.2.2 Ensure IP forwarding is disabled	Fail
	3.3 Network Parameters (Host and Router)	
1.0	3.3.1 Ensure source routed packets are not accepted	Fail
1.0	3.3.2 Ensure ICMP redirects are not accepted	Fail
1.0	3.3.3 Ensure secure ICMP redirects are not accepted	Fail
1.0	3.3.4 Ensure suspicious packets are logged	Fail
1.0	3.3.5 Ensure broadcast ICMP requests are ignored	Fail
1.0	3.3.6 Ensure bogus ICMP responses are ignored	Fail
1.0	3.3.7 Ensure Reverse Path Filtering is enabled	Fail
1.0	3.3.8 Ensure TCP SYN Cookies is enabled	Fail
1.0	3.3.9 Ensure IPv6 router advertisements are not accepted	Fail
	3.4 Firewall Configuration	
	3.4.1 Configure UncomplicatedFirewall	
1.0	3.4.1.1 Ensure ufw is installed	Fail
1.0	3.4.1.2 Ensure iptables-persistent is not installed with ufw	Pass

w	Benchmark Item	Result
1.0	3.4.1.3 Ensure ufw service is enabled	Fail
1.0	3.4.1.4 Ensure ufw loopback traffic is configured	Fail
	3.4.1.5 Ensure ufw outbound connections are configured	Manual
1.0	3.4.1.6 Ensure ufw firewall rules exist for all open ports	Fail
1.0	3.4.1.7 Ensure ufw default deny firewall policy	Fail
	3.4.2 Configure nftables	
1.0	3.4.2.1 Ensure nftables is installed	Fail
1.0	3.4.2.2 Ensure ufw is uninstalled or disabled with nftables	Pass
	3.4.2.3 Ensure iptables are flushed with nftables	Manual
1.0	3.4.2.4 Ensure a nftables table exists	Fail
1.0	3.4.2.5 Ensure nftables base chains exist	Fail
1.0	3.4.2.6 Ensure nftables loopback traffic is configured	Fail
	3.4.2.7 Ensure nftables outbound and established connections are configured	Manual
1.0	3.4.2.8 Ensure nftables default deny firewall policy	Fail
1.0	3.4.2.9 Ensure nftables service is enabled	Fail
1.0	3.4.2.10 Ensure nftables rules are permanent	Fail
	3.4.3 Configure iptables	
	3.4.3.1 Configure iptables software	
1.0	3.4.3.1.1 Ensure iptables packages are installed	Fail
1.0	3.4.3.1.2 Ensure nftables is not installed with iptables	Pass
1.0	3.4.3.1.3 Ensure ufw is uninstalled or disabled with iptables	Pass
	3.4.3.2 Configure IPv4 iptables	
1.0	3.4.3.2.1 Ensure iptables default deny firewall policy	Fail
1.0	3.4.3.2.2 Ensure iptables loopback traffic is configured	Fail
	3.4.3.2.3 Ensure iptables outbound and established connections are configured	Manual
1.0	3.4.3.2.4 Ensure iptables firewall rules exist for all open ports	Fail
	3.4.3.3 Configure IPv6 ip6tables	
1.0	3.4.3.3.1 Ensure ip6tables default deny firewall policy	Fail
1.0	3.4.3.3.2 Ensure ip6tables loopback traffic is configured	Pass
	3.4.3.3.3 Ensure ip6tables outbound and established connections are configured	Manual
1.0	3.4.3.3.4 Ensure ip6tables firewall rules exist for all open ports	Fail
	4 Access, Authentication and Authorization	
	4.1 Configure time-based job schedulers	
1.0	4.1.1 Ensure cron daemon is enabled and active	Pass
1.0	4.1.2 Ensure permissions on /etc/crontab are configured	Pass
1.0	4.1.3 Ensure permissions on /etc/cron.hourly are configured	Fail
1.0	4.1.4 Ensure permissions on /etc/cron.daily are configured	Fail
1.0	4.1.5 Ensure permissions on /etc/cron.weekly are configured	Fail
1.0	4.1.6 Ensure permissions on /etc/cron.monthly are configured	Fail
1.0	4.1.7 Ensure permissions on /etc/cron.d are configured	Fail
1.0	4.1.8 Ensure cron is restricted to authorized users	Fail
1.0	4.1.9 Ensure at is restricted to authorized users	Pass
	4.2 Configure SSH Server	
1.0	4.2.1 Ensure permissions on /etc/ssh/sshd_config are configured	Fail
1.0	4.2.2 Ensure permissions on SSH private host key files are configured	Pass
1.0	4.2.3 Ensure permissions on SSH public host key files are configured	Pass
1.0	4.2.4 Ensure SSH access is limited	Fail
1.0	4.2.5 Ensure SSH LogLevel is appropriate	Pass
1.0	4.2.6 Ensure SSH PAM is enabled	Pass
1.0	4.2.7 Ensure SSH root login is disabled	Fail
1.0	4.2.8 Ensure SSH HostbasedAuthentication is disabled	Pass
1.0	4.2.9 Ensure SSH PermitEmptyPasswords is disabled	Pass
1.0	4.2.10 Ensure SSH PermitUserEnvironment is disabled	Pass
1.0	4.2.11 Ensure SSH IgnoreRhosts is enabled	Pass
1.0	4.2.13 Ensure only strong Ciphers are used	Pass
1.0	4.2.14 Ensure only strong MAC algorithms are used	Pass
1.0	4.2.15 Ensure only strong Key Exchange algorithms are used	Pass

w	Benchmark Item	Result
1.0	4.2.17 Ensure SSH warning banner is configured	Pass
1.0	4.2.18 Ensure SSH MaxAuthTries is set to 4 or less	Fail
1.0	4.2.19 Ensure SSH MaxStartups is configured	Fail
1.0	4.2.20 Ensure SSH LoginGraceTime is set to one minute or less	Fail
1.0	4.2.21 Ensure SSH MaxSessions is set to 10 or less	Pass
1.0	4.2.22 Ensure SSH Idle Timeout Interval is configured	Pass
	4.3 Configure privilege escalation	
1.0	4.3.1 Ensure sudo is installed	Pass
1.0	4.3.2 Ensure sudo commands use pty	Fail
1.0	4.3.3 Ensure sudo log file exists	Fail
1.0	4.3.5 Ensure re-authentication for privilege escalation is not disabled globally	Pass
1.0	4.3.6 Ensure sudo authentication timeout is configured correctly	Pass
1.0	4.3.7 Ensure access to the su command is restricted	Fail
	4.4 Configure PAM	
1.0	4.4.1 Ensure password creation requirements are configured	Fail
1.0	4.4.2 Ensure lockout for failed password attempts is configured	Fail
1.0	4.4.3 Ensure password reuse is limited	Fail
1.0	4.4.4 Ensure strong password hashing algorithm is configured	Pass
	4.4.5 Ensure all current passwords uses the configured hashing algorithm	Manual
	4.5 User Accounts and Environment	
	4.5.1 Set Shadow Password Suite Parameters	
1.0	4.5.1.1 Ensure minimum days between password changes is configured	Fail
1.0	4.5.1.2 Ensure password expiration is 365 days or less	Fail
1.0	4.5.1.3 Ensure password expiration warning days is 7 or more	Pass
1.0	4.5.1.4 Ensure inactive password lock is 30 days or less	Fail
1.0	4.5.1.5 Ensure all users last password change date is in the past	Pass
1.0	4.5.1.6 Ensure the number of changed characters in a new password is configured	Fail
1.0	4.5.1.7 Ensure preventing the use of dictionary words for passwords is configured	Fail
1.0	4.5.2 Ensure system accounts are secured	Pass
1.0	4.5.3 Ensure default group for the root account is GID 0	Pass
1.0	4.5.4 Ensure default user umask is 027 or more restrictive	Fail
1.0	4.5.5 Ensure default user shell timeout is configured	Fail
1.0	4.5.7 Ensure maximum number of same consecutive characters in a password is configured	Fail
	5 Logging and Auditing	
	5.1 Configure Logging	
	5.1.1 Configure journald	
	5.1.1.1 Ensure journald is configured to send logs to a remote log host	
1.0	5.1.1.1.1 Ensure systemd-journal-remote is installed	Pass
	5.1.1.1.2 Ensure systemd-journal-remote is configured	Manual
	5.1.1.1.3 Ensure systemd-journal-remote is enabled	Manual
1.0	5.1.1.1.4 Ensure journald is not configured to receive logs from a remote client	Pass
1.0	5.1.1.2 Ensure journald service is enabled	Pass
1.0	5.1.1.3 Ensure journald is configured to compress large log files	Fail
1.0	5.1.1.4 Ensure journald is configured to write logfiles to persistent disk	Fail
	5.1.1.5 Ensure journald is not configured to send logs to rsyslog	Manual
	5.1.1.6 Ensure journald log rotation is configured per site policy	Manual
	5.1.1.7 Ensure journald default file permissions configured	Manual
	5.1.2 Configure rsyslog	
1.0	5.1.2.1 Ensure rsyslog is installed	Pass
1.0	5.1.2.2 Ensure rsyslog service is enabled	Pass
	5.1.2.3 Ensure journald is configured to send logs to rsyslog	Manual
1.0	5.1.2.4 Ensure rsyslog default file permissions are configured	Pass
	5.1.2.5 Ensure logging is configured	Manual
	5.1.2.6 Ensure rsyslog is configured to send logs to a remote log host	Manual
1.0	5.1.2.7 Ensure rsyslog is not configured to receive logs from a remote client	Pass

w	Benchmark Item	Result
1.0	5.1.3 Ensure all logfiles have appropriate access configured	Fail
	5.2 Configure System Accounting (auditd)	
	5.2.1 Ensure auditing is enabled	
	5.2.2 Configure Data Retention	
	5.2.3 Configure auditd rules	
	5.2.4 Configure auditd file access	
1.0	5.2.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools	Fail
	6 System Maintenance	
	6.1 System File Permissions	
1.0	6.1.1 Ensure permissions on /etc/passwd are configured	Pass
1.0	6.1.2 Ensure permissions on /etc/passwd- are configured	Pass
1.0	6.1.3 Ensure permissions on /etc/group are configured	Pass
1.0	6.1.4 Ensure permissions on /etc/group- are configured	Pass
1.0	6.1.5 Ensure permissions on /etc/shadow are configured	Pass
1.0	6.1.6 Ensure permissions on /etc/shadow- are configured	Pass
1.0	6.1.7 Ensure permissions on /etc/gshadow are configured	Pass
1.0	6.1.8 Ensure permissions on /etc/gshadow- are configured	Pass
1.0	6.1.9 Ensure permissions on /etc/shells are configured	Pass
1.0	6.1.10 Ensure permissions on /etc/opasswd are configured	Fail
1.0	6.1.11 Ensure world writable files and directories are secured	Fail
1.0	6.1.12 Ensure no unowned or ungrouped files or directories exist	Fail
	6.1.13 Ensure SUID and SGID files are reviewed	Manual
	6.2 Local User and Group Settings	
1.0	6.2.1 Ensure accounts in /etc/passwd use shadowed passwords	Pass
1.0	6.2.2 Ensure /etc/shadow password fields are not empty	Pass
1.0	6.2.3 Ensure all groups in /etc/passwd exist in /etc/group	Pass
1.0	6.2.4 Ensure shadow group is empty	Pass
1.0	6.2.5 Ensure no duplicate UIDs exist	Pass
1.0	6.2.6 Ensure no duplicate GIDs exist	Pass
1.0	6.2.7 Ensure no duplicate user names exist	Pass
1.0	6.2.8 Ensure no duplicate group names exist	Pass
1.0	6.2.9 Ensure root PATH Integrity	Pass
1.0	6.2.10 Ensure root is the only UID 0 account	Pass
1.0	6.2.11 Ensure local interactive user home directories are configured	Fail
1.0	6.2.12 Ensure local interactive user dot files access is configured	Fail

⇧

Assessment Details

1 Initial Setup

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

1.1 Filesystem Configuration

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

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

Note: If you are repartitioning a system that has already been installed (This may require the system to be in single-user mode):

- Mount the new partition to a temporary mountpoint e.g. `mount /dev/sda2 /mnt`
- Copy data from the original partition to the new partition. e.g. `cp /var/tmp/* /mnt`
- Verify that all data is present on the new partition. e.g. `ls -la /mnt`
- Unmount the new partition. e.g. `umount /mnt`
- Remove the data from the original directory that was in the old partition. e.g. `rm -Rf /var/tmp/*` Otherwise it will still consume space in the old partition that will be masked when the new filesystem is mounted.

- Mount the new partition to the desired mountpoint. e.g. `mount /dev/sda2 /var/tmp`
- Update `/etc/fstab` with the new mountpoint. e.g. `/dev/sda2 /var/tmp xfs defaults,rw,nosuid,nodev,noexec,relatime 0 0`

1.1.1 Disable unused filesystems

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

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

Note : This should not be considered a comprehensive list of filesystems. You may wish to consider additions to those listed here for your environment. For the current available file system modules on the system see `/usr/lib/modules/$(uname -r)/kernel/fs`

Start up scripts

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

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

Return values

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

1.1.1.1 Ensure mounting of cramfs filesystems is disabled

Fail

Description:

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

Rationale:

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

Remediation:

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

If the module is available in the running kernel:

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

If available in ANY installed kernel:

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

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

- No remediation is necessary

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



{
```

```
l_mname="cramfs" # set module name

l_mtype="fs" # set module type

l_mpath="/lib/modules/**/kernel/$l_mtype"

l_mpname="$(tr '-' '_' <<< "$l_mname")"

l_mndir="$(tr '-' '/' <<< "$l_mname")"


module_loadable_fix()

{

# If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"

l_loadable="$(modprobe -n -v "$l_mname")"

[ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P -- "(^\h*install|\b$l_mname)\b" <<<
"$l_loadable")"

if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then

echo -e "\n - setting module: \"$l_mname\" to be not loadable"

echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf

fi

}

module_loaded_fix()

{

# If the module is currently loaded, unload the module

if lsmod | grep "$l_mname" > /dev/null 2>&1; then

echo -e "\n - unloading module \"$l_mname\""

modprobe -r "$l_mname"

fi

}

module_deny_fix()

{

# If the module isn't deny listed, denylist the module

if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then

echo -e "\n - deny listing \"$l_mname\""

echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf

fi

}

# Check if the module exists on the system

for l_mdir in $l_mpath; do

if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then

echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."

module_deny_fix

if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then

module_loadable_fix

module_loaded_fix

fi

else
```

```
echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"

fi

done

echo -e "\n - remediation of module: \"$l_mname\" complete\n"

}
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

1.1.1.2 Ensure mounting of freevxfs filesystems is disabled

Fail

Description:

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

Rationale:

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

Remediation:

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

If the module is available in the running kernel:

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

If available in ANY installed kernel:

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

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

- No remediation is necessary

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



{

l_mname="freevxfs" # set module name

l_mtype="fs" # set module type

l_mpath="/lib/modules/**/kernel/$l_mtype"

l_mpname="$(tr '-' '_' <<< "$l_mname")"

l_mndir="$(tr '-' '/' <<< "$l_mname")"
```

```
module_loadable_fix()

{

# If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"

l_loadable="$(modprobe -n -v "$l_mname")"

[ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P -- "(^\h*install|\b$l_mname)\b" <<<
"$l_loadable")"

if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then

echo -e "\n - setting module: \"$l_mname\" to be not loadable"

echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf

fi

}

module_loaded_fix()

{

# If the module is currently loaded, unload the module

if lsmod | grep "$l_mname" > /dev/null 2>&1; then

echo -e "\n - unloading module \"$l_mname\""

modprobe -r "$l_mname"

fi

}

module_deny_fix()

{

# If the module isn't deny listed, denylist the module

if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then

echo -e "\n - deny listing \"$l_mname\""

echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf

fi

}

# Check if the module exists on the system

for l_mdir in $l_mpath; do

if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then

echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."

module_deny_fix

if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then

module_loadable_fix

module_loaded_fix

fi

else

echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"

fi

done

echo -e "\n - remediation of module: \"$l_mname\" complete\n"

}
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

1.1.1.3 Ensure mounting of jffs2 filesystems is disabled

Fail

Description:

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

Rationale:

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

Remediation:

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

If the module is available in the running kernel:

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

If available in ANY installed kernel:

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

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

- No remediation is necessary

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



{

l_mname="jffs2" # set module name

l_mtype="fs" # set module type

l_mpath="/lib/modules/**/kernel/$l_mtype"

l_mpname="$(tr '-' '_' <<< "$l_mname")"

l_mndir="$(tr '-' '/' <<< "$l_mname")"



module_loadable_fix()

{

# If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"

l_loadable="$(modprobe -n -v "$l_mname")"

[ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P -- "(^\h*install|\b$l_mname)\b" <<<
"$l_loadable")"

if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
```

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

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

1.1.1.4 Ensure mounting of hfs filesystems is disabled

Fail

Description:

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

Rationale:

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

Remediation:

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

If the module is available in the running kernel:

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

If available in ANY installed kernel:

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

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

- No remediation is necessary

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



{

l_mname="hfs" # set module name

l_mtype="fs" # set module type

l_mpath="/lib/modules/**/kernel/$l_mtype"

l_mpname="$(tr '-' '_' <<< "$l_mname")"

l_mndir="$(tr '-' '/' <<< "$l_mname")"



module_loadable_fix()

{

# If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"

l_loadable="$(modprobe -n -v "$l_mname")"

[ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P -- "(^\h*install|\b$l_mname)\b" <<<
"$l_loadable")"

if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then

echo -e "\n - setting module: \"$l_mname\" to be not loadable"

echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf

fi

}

module_loaded_fix()

{

# If the module is currently loaded, unload the module
```

```
if lsmod | grep "$l_mname" > /dev/null 2>&1; then
echo -e "\n - unloading module \"$l_mname\""
modprobe -r "$l_mname"
fi
}
module_deny_fix()
{
# If the module isn't deny listed, denylist the module
if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
echo -e "\n - deny listing \"$l_mname\""
echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
fi
}
# Check if the module exists on the system
for l_mdir in $l_mpath; do
if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
module_deny_fix
if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
module_loadable_fix
module_loaded_fix
fi
else
echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
fi
done
echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

1.1.1.5 Ensure mounting of hfsplus filesystems is disabled

Fail

Description:

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

Rationale:

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

Remediation:

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

If the module is available in the running kernel:

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

If available in ANY installed kernel:

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

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

- No remediation is necessary

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



{

l_mname="hfsplus" # set module name

l_mtype="fs" # set module type

l_mpath="/lib/modules/**/kernel/$l_mtype"

l_mpname="$(tr '-' '_' <<< "$l_mname")"

l_mndir="$(tr '-' '/' <<< "$l_mname")"



module_loadable_fix()

{

# If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"

l_loadable="$(modprobe -n -v "$l_mname")"

[ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P -- "(^\h*install|\b$l_mname)\b" <<<
"$l_loadable")"

if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then

echo -e "\n - setting module: \"$l_mname\" to be not loadable"

echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf

fi

}

module_loaded_fix()

{

# If the module is currently loaded, unload the module

if lsmod | grep "$l_mname" > /dev/null 2>&1; then

echo -e "\n - unloading module \"$l_mname\""

modprobe -r "$l_mname"

fi

}

module_deny_fix()
```

```
{
# If the module isn't deny listed, denylist the module
if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
echo -e "\n - deny listing \"$l_mname\""
echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
fi
}
# Check if the module exists on the system
for l_mdir in $l_mpath; do
if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
module_deny_fix
if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
module_loadable_fix
module_loaded_fix
fi
else
echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
fi
done
echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

1.1.2 Configure /tmp

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

1.1.2.1 Ensure /tmp is a separate partition — Fail

Description:

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

Rationale:

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

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

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

Remediation:

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

Using `/etc/fstab` :

Configure `/etc/fstab` as appropriate:

Example:

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

-OR-

Using a `tmp.mount` unit file:

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

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

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

Example:

```
# SPDX-License-Identifier: LGPL-2.1+

#

# 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=https://systemd.io/TEMPORARY_DIRECTORIES

Documentation=man:file-hierarchy(7)

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

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,noexec
```

```
[Install]

WantedBy=local-fs.target
```

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

```
# systemctl daemon-reload
```

Run the following command to enable and start tmp.mount

```
# systemctl --now enable tmp.mount
```

Note: A reboot may be required to transition to `/tmp` mounted to `tmpfs`

Impact:

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

Running out of `/tmp` space is a problem regardless of what kind of filesystem lies under it, but in a configuration where `/tmp` is not a separate file system it will essentially have the whole disk available, as the default installation only creates a single `/` partition. On the other hand, a RAM-based `/tmp` (as with `tmpfs`) will almost certainly be much smaller, which can lead to applications filling up the filesystem much more easily. Another alternative is to create a dedicated partition for `/tmp` from a separate volume or disk. One of the downsides of a disk-based dedicated partition is that it will be slower than `tmpfs` which is RAM-based.

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/
- **URL:** https://www.freedesktop.org/software/systemd/man/systemd-fstab-generator.html
- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.2.2 Ensure nodev option set on /tmp partition

Pass

Description:

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

Rationale:

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

Remediation:

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

Example:

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

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

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

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.2.3 Ensure noexec option set on /tmp partition

Pass

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` .

Remediation:

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

Example:

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

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

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

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.2.4 Ensure nosuid option set on /tmp partition

Pass

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` .

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.3 Configure /var

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

1.1.3.2 Ensure nodev option set on /var partition

Pass

Description:

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

Rationale:

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

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.3.3 Ensure nosuid option set on /var partition

Pass

Description:

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

Rationale:

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

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.4 Configure /var/tmp

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

1.1.4.2 Ensure nodev option set on /var/tmp partition

Pass

Description:

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

Rationale:

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

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.4.3 Ensure noexec option set on /var/tmp partition

Pass

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` .

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

>

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
>

Back to Summary

1.1.4.4 Ensure nosuid option set on /var/tmp partition

Pass

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` .

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
>

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
>

Back to Summary

1.1.5 Configure /var/log

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

1.1.5.2 Ensure nodev option set on /var/log partition

Pass

Description:

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

Rationale:

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

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
  >

Back to Summary

1.1.5.3 Ensure noexec option set on /var/log partition

Pass

Description:

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

Rationale:

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

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
  >

Back to Summary

1.1.5.4 Ensure nosuid option set on /var/log partition

Pass

Description:

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

Rationale:

Since the `/var/log` filesystem is only intended for log files, set this option to ensure that users cannot create `setuid` files in `/var/log` .

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.6 Configure /var/log/audit

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

1.1.6.2 Ensure nodev option set on /var/log/audit partition

Pass

Description:

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

Rationale:

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

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.6.3 Ensure noexec option set on /var/log/audit partition

Pass

Description:

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

Rationale:

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

Remediation:

IF the `/var/log/audit` partition exists, edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var` partition.

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: CM-11

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.6.4 Ensure nosuid option set on /var/log/audit partition

Pass

Description:

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

Rationale:

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

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: CM-6

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.7 Configure /home

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

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

1.1.7.2 Ensure nodev option set on /home partition

Pass

Description:

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

Rationale:

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

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.7.3 Ensure nosuid option set on /home partition

Pass

Description:

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

Rationale:

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

Remediation:

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

Example:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.8 Configure /dev/shm

1.1.8.1 Ensure nodev option set on /dev/shm partition

Pass

Description:

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

Rationale:

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

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.

Example:

```
tmpfs /dev/shm tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.8.2 Ensure noexec option set on /dev/shm partition

Pass

Description:

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

Rationale:

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

Remediation:

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

Example:

```
tmpfs /dev/shm tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the fstab(5) manual page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.8.3 Ensure nosuid option set on /dev/shm partition

Pass

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.

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.

Example:

```
tmpfs /dev/shm tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.1.9 Disable Automounting

Pass

Description:

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

Rationale:

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

Remediation:

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

```
# apt purge autofs
```

-OR- if there are dependencies on the autofs package:

Run the following commands to mask `autofs` :

```
# systemctl stop autofs

# systemctl mask autofs
```

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 are considered adequate there is little value add in turning off automounting.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More >

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More >

Back to Summary

1.1.10 Disable USB Storage

Fail

Description:

USB storage provides a means to transfer and store files insuring persistence and availability of the files independent of network connection status. Its popularity and utility has led to USB-based malware being a simple and common means for network infiltration and a first step to establishing a persistent threat within a networked environment.

Rationale:

Restricting USB access on the system will decrease the physical attack surface for a device and diminish the possible vectors to introduce malware.

Remediation:

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

If the module is available in the running kernel:

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

If available in ANY installed kernel:

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

If the kernel module is not available on the system:

- No remediation is necessary

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

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

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

```
echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
fi
done
echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

Impact:

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SI-3

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More
- **Control 13: Data Protection:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
  >

Back to Summary

1.2 Filesystem Integrity Checking

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

1.2.1 Ensure AIDE is installed

Fail

Description:

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

Rationale:

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

Remediation:

Install AIDE using the appropriate package manager or manual installation:

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

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

Run the following commands to initialize AIDE:

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.2.2 Ensure filesystem integrity is regularly checked

Fail

Description:

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

Rationale:

Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

Remediation:

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

Run the following command:

```
# crontab -u root -e
```

Add the following line to the crontab:

```
0 5 * * * /usr/bin/aide.wrapper --config /etc/aide/aide.conf --check
```

OR If aidecheck.service and aidecheck.timer will be used to schedule and run aide check:

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

```
[Unit]
Description=Aide Check

[Service]
Type=simple
ExecStart=/usr/bin/aide.wrapper --config /etc/aide/aide.conf --check

[Install]
WantedBy=multi-user.target
```

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

```
[Unit]
Description=Aide check every day at 5AM

[Timer]
OnCalendar=*-*-* 05:00:00
Unit=aidecheck.service
```

```
[Install]

WantedBy=multi-user.target
```

Run the following commands:

```
# chown root:root /etc/systemd/system/aidecheck.*

# chmod 0644 /etc/systemd/system/aidecheck.*



# systemctl daemon-reload



# systemctl enable aidecheck.service

# systemctl --now enable aidecheck.timer
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.service
- **URL:** https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.timer
- **URL:** NIST SP 800-53 Rev. 5: AU-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

1.3 Configure Software and Patch Management

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

Software updates often offer new and improved features and speed enhancements

1.3.1 Ensure updates, patches, and additional security software are installed

Manual

Description:

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

Rationale:

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

Remediation:

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

```
# apt upgrade
```

OR

```
# apt dist-upgrade
```

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SI-2

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More >

CIS Critical Security Controls V8.0:

- **Control 7: Continuous Vulnerability Management:** -- More >

Back to Summary

1.3.2 Ensure package manager repositories are configured

Manual

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.

Remediation:

Configure your package manager repositories according to site policy.

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SI-2

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More >

CIS Critical Security Controls V8.0:

- **Control 7: Continuous Vulnerability Management:** -- More >

Back to Summary

1.3.3 Ensure GPG keys are configured

Manual

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.

Remediation:

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

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SI-2

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 7: Continuous Vulnerability Management:** -- More
  >

Back to Summary

1.4 Secure Boot Settings

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

1.4.1 Ensure bootloader password is set

Fail

Description:

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

Rationale:

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

Remediation:

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

```
# grub-mkpasswd-pbkdf2


Enter password: <password>

Reenter password: <password>

PBKDF2 hash of your password is <encrypted-password>
```

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

```
cat <<EOF

set superusers="<username>"

password_pbkdf2 <username> <encrypted-password>

EOF
```

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

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

Example:

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

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

```
# update-grub
```

Impact:

If password protection is enabled, only the designated superuser can edit a GRUB 2 menu item by pressing "e" or access the GRUB 2 command line by pressing "c"

If GRUB 2 is set up to boot automatically to a password-protected menu entry the user has no option to back out of the password prompt to select another menu entry. Holding the SHIFT key will not display the menu in this case. The user must enter the correct username and password. If unable to do so, the configuration files will have to be edited via a LiveCD or other means to fix the problem

You can add `--unrestricted` to the menu entries to allow the system to boot without entering a password. A password will still be required to edit menu items.

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-6

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

1.4.2 Ensure permissions on bootloader config are configured

Fail

Description:

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

Rationale:

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

Remediation:

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

```
# chown root:root /boot/grub/grub.cfg

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-6

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.4.3 Ensure authentication required for single user mode

Pass

Description:

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

Rationale:

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

Remediation:

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

```
# passwd root
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: IA-5

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

1.5 Additional Process Hardening

1.5.1 Ensure prelink is not installed

Pass

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.

Remediation:

Run the following command to restore binaries to normal:

```
# prelink -ua
```

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

```
# apt purge prelink
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
  >

Back to Summary

1.5.2 Ensure address space layout randomization (ASLR) is enabled

Fail

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.

Remediation:

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

- `kernel.randomize_va_space = 2`

Example:

```
# printf "

kernel.randomize_va_space = 2

" >> /etc/sysctl.d/60-kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
  >

Back to Summary

1.5.3 Ensure ptrace_scope is restricted

Pass

Description:

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

Rationale:

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

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

Remediation:

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

- `kernel.yama.ptrace_scope = 1`

Example:

```
# printf "

kernel.yama.ptrace_scope = 1

" >> /etc/sysctl.d/60-kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://www.kernel.org/doc/Documentation/security/Yama.txt
- **URL:** https://github.com/raj3shp/termspy

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

1.5.4 Ensure Automatic Error Reporting is not enabled

Pass

Description:

The Apport Error Reporting Service automatically generates crash reports for debugging

Rationale:

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

Remediation:

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

```
enabled=0
```

Run the following commands to stop and disable the apport service

```
# systemctl stop apport.service

# systemctl --now disable apport.service
```

-- OR --

Run the following command to remove the apport package:

```
# apt purge apport
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

1.5.5 Ensure core dumps are restricted

Fail

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.

Remediation:

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

```
* hard core 0
```

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

- `fs.suid_dumpable = 0`

Example:

```
# printf "

fs.suid_dumpable = 0

" >> /etc/sysctl.d/60-fs_sysctl.conf
```

Run the following command to set the active kernel parameter:

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

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

-IF- systemd-coredump is installed:

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

```
Storage=none

ProcessSizeMax=0
```

Run the command:

```
systemctl daemon-reload
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

Back to Summary

1.6 Mandatory Access Control

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

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

Note:

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

1.6.1 Configure AppArmor

AppArmor provides a Mandatory Access Control (MAC) system that greatly augments the default Discretionary Access Control (DAC) model. Under AppArmor MAC rules are applied by file paths instead of by security contexts as in other MAC systems. As such it does not require support in the filesystem and can be applied to network mounted filesystems for example. AppArmor security policies define what system resources applications can access and what privileges they can do so with. This automatically limits the damage that the software can do to files accessible by the calling user. The user does not need to take any action to gain this benefit. For an action to occur, both the traditional DAC permissions must be satisfied as well as the AppArmor MAC rules. The action will not be allowed if either one of these models does not permit the action. In this way, AppArmor rules can only make a system's permissions more restrictive and secure.

References:

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

1.6.1.1 Ensure AppArmor is installed

Fail

Description:

AppArmor provides Mandatory Access Controls.

Rationale:

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

Remediation:

Install AppArmor.

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.6.1.2 Ensure AppArmor is enabled in the bootloader configuration

Fail

Description:

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

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

Rationale:

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

Remediation:

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

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

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

```
# update-grub
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AC-3

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.6.1.3 Ensure all AppArmor Profiles are in enforce or complain mode

Fail

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.

Remediation:

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

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

OR

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AC-3

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.7 Command Line Warning Banners

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

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

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

1.7.1 Ensure message of the day is configured properly

Pass

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.

Remediation:

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

Example Text:

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

-- OR --

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

Run the following command to remove the motd file:

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-3

Back to Summary

1.7.2 Ensure local login warning banner is configured properly

Pass

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.

Remediation:

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

Example Text:

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

Back to Summary

1.7.3 Ensure remote login warning banner is configured properly

Fail

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.

Remediation:

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

Example Text:

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

Back to Summary

1.7.4 Ensure permissions on /etc/motd are configured

Pass

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.

Remediation:

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

```
# chown root:root $(readlink -e /etc/motd)

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

-- OR --

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
>

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
>

Back to Summary

1.7.5 Ensure permissions on /etc/issue are configured

Pass

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.

Remediation:

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

```
# chown root:root $(readlink -e /etc/issue)

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

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.7.6 Ensure permissions on /etc/issue.net are configured

Pass

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.

Remediation:

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

```
# chown root:root $(readlink -e /etc/issue.net)

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

1.8 GNOME Display Manager

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

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

1.8.2 Ensure GDM login banner is configured

Pass

Description:

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

Rationale:

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

Remediation:

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

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



{

l_pkgoutput=""

if command -v dpkg-query > /dev/null 2>&1; then

l_pq="dpkg-query -W"

elif command -v rpm > /dev/null 2>&1; then

l_pq="rpm -q"

fi

l_pcl="gdm gdm3" # Space seporated list of packages to check

for l_pn in $l_pcl; do

$l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists on the
system\n - checking configuration"

done

if [ -n "$l_pkgoutput" ]; then



l_gdmprofile="gdm" # Set this to desired profile name IaW Local site policy

l_bmessage="'Authorized uses only. All activity may be monitored and reported'" # Set to desired banner
message

if [ ! -f "/etc/dconf/profile/$l_gdmprofile" ]; then

echo "Creating profile \"$l_gdmprofile\""

echo -e "user-db:user\nsystem-db:$l_gdmprofile\nfile-db:/usr/share/$l_gdmprofile/greeter-dconf-defaults"
> /etc/dconf/profile/$l_gdmprofile

fi

if [ ! -d "/etc/dconf/db/$l_gdmprofile.d/" ]; then

echo "Creating dconf database directory \"/etc/dconf/db/$l_gdmprofile.d/\""

mkdir /etc/dconf/db/$l_gdmprofile.d/

fi

if ! grep -Piq '^\h*banner-message-enable\h*=\h*true\b' /etc/dconf/db/$l_gdmprofile.d/*; then

echo "creating gdm keyfile for machine-wide settings"

if ! grep -Piq -- '^\h*banner-message-enable\h*=\h*' /etc/dconf/db/$l_gdmprofile.d/*; then

l_kfile="/etc/dconf/db/$l_gdmprofile.d/01-banner-message"

echo -e "\n[org/gnome/login-screen]\nbanner-message-enable=true" >> "$l_kfile"

else

l_kfile="$(grep -Pil -- '^\h*banner-message-enable\h*=\h*' /etc/dconf/db/$l_gdmprofile.d/*)"

! grep -Pq '^\h*\[org\/gnome\/login-screen\]' "$l_kfile" && sed -ri '/^\s*banner-message-enable/ i\
[org/gnome/login-screen]' "$l_kfile"

! grep -Pq '^\h*banner-message-enable\h*=\h*true\b' "$l_kfile" && sed -ri 's/^\s*(banner-message-
enable\s*=\s*)(\S+)(\s*.*$)/\1true \3//' "$l_kfile"

# sed -ri '/^\s*\[org\/gnome\/login-screen\]/ a\\nbanner-message-enable=true' "$l_kfile"

fi

fi
```

```
if ! grep -Piq "^\h*banner-message-text=[\'\"]+\S+" "$l_kfile"; then

sed -ri "/^\s*banner-message-enable/ a\banner-message-text=$l_bmessage" "$l_kfile"

fi

dconf update

else

echo -e "\n\n - GNOME Desktop Manager isn't installed\n - Recommendation is Not Applicable\n - No
remediation required\n"

fi

}
```

Note:

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

OR

Run the following command to remove the gdm3 package:

```
# apt purge gdm3
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

Back to Summary

1.8.3 Ensure GDM disable-user-list option is enabled

Pass

Description:

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

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

Rationale:

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

Remediation:

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

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

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



{

l_gdmprofile="gdm"

if [ ! -f "/etc/dconf/profile/$l_gdmprofile" ]; then

echo "Creating profile \"$l_gdmprofile\""

echo -e "user-db:user\nsystem-db:$l_gdmprofile\nfile-db:/usr/share/$l_gdmprofile/greeter-dconf-defaults"
> /etc/dconf/profile/$l_gdmprofile

fi
```

```
if [ ! -d "/etc/dconf/db/$l_gdmprofile.d/" ]; then

echo "Creating dconf database directory \"/etc/dconf/db/$l_gdmprofile.d/\""

mkdir /etc/dconf/db/$l_gdmprofile.d/

fi

if ! grep -Piq '^\h*disable-user-list\h*=\h*true\b' /etc/dconf/db/$l_gdmprofile.d/*; then

echo "creating gdm keyfile for machine-wide settings"

if ! grep -Piq -- '^\h*\[org\/gnome\/login-screen\]' /etc/dconf/db/$l_gdmprofile.d/*; then

echo -e "\n[org/gnome/login-screen]\n# Do not show the user list\ndisable-user-list=true" >>
/etc/dconf/db/$l_gdmprofile.d/00-login-screen

else

sed -ri '/^\s*\[org\/gnome\/login-screen\]/ a\# Do not show the user list\ndisable-user-list=true'
$(grep -Pil -- '^\h*\[org\/gnome\/login-screen\]' /etc/dconf/db/$l_gdmprofile.d/*)

fi

fi

dconf update

}
```

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

OR

Run the following command to remove the GNOME package:

```
# apt purge gdm3
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

Back to Summary

1.8.4 Ensure GDM screen locks when the user is idle

Pass

Description:

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

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

Example key file:

```
# Specify the dconf path

[org/gnome/desktop/session]



# Number of seconds of inactivity before the screen goes blank

# Set to 0 seconds if you want to deactivate the screensaver.

idle-delay=uint32 900



# Specify the dconf path

[org/gnome/desktop/screensaver]
```

```
# Number of seconds after the screen is blank before locking the screen

lock-delay=uint32 5
```

Rationale:

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

Remediation:

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

```
user-db:user

system-db:{NAME_OF_DCONF_DATABASE}
```

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

Example:

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

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

Example:

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

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

Example script:

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



{

l_key_file="/etc/dconf/db/local.d/00-screensaver"

l_idmv="900" # Set max value for idle-delay in seconds (between 1 and 900)

l_ldmv="5" # Set max value for lock-delay in seconds (between 0 and 5)

{

echo '# Specify the dconf path'

echo '[org/gnome/desktop/session]'

echo ''

echo '# Number of seconds of inactivity before the screen goes blank'

echo '# Set to 0 seconds if you want to deactivate the screensaver.'

echo "idle-delay=uint32 $l_idmv"

echo ''

echo '# Specify the dconf path'

echo '[org/gnome/desktop/screensaver]'

echo ''

echo '# Number of seconds after the screen is blank before locking the screen'

echo "lock-delay=uint32 $l_ldmv"

} > "$l_key_file"

}
```

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

Run the following command to update the system databases:

```
# dconf update
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://help.gnome.org/admin/system-admin-guide/stable/desktop-lockscreen.html.en
- **URL:** NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

1.8.5 Ensure GDM screen locks cannot be overridden

Pass

Description:

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

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

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

Example Lock File:

```
# Lock desktop screensaver settings

/org/gnome/desktop/session/idle-delay

/org/gnome/desktop/screensaver/lock-delay
```

Rationale:

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

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

Remediation:

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

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



{

# Check if GNMOE Desktop Manager is installed. If package isn't installed, recommendation is Not
Applicable\n

# determine system's package manager

l_pkgoutput=""

if command -v dpkg-query > /dev/null 2>&1; then

l_pq="dpkg-query -W"

elif command -v rpm > /dev/null 2>&1; then

l_pq="rpm -q"

fi
```

```
# Check if GDM is installed

l_pcl="gdm gdm3" # Space seporated list of packages to check

for l_pn in $l_pcl; do

$l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="y" && echo -e "\n - Package: \"$l_pn\" exists on the
system\n - remediating configuration if needed"

done

# Check configuration (If applicable)

if [ -n "$l_pkgoutput" ]; then

# Look for idle-delay to determine profile in use, needed for remaining tests

l_kfd="/etc/dconf/db/$(grep -Psril '^\h*idle-delay\h*=\h*uint32\h+\d+\b' /etc/dconf/db/*/ | awk -F'/'
'{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked

# Look for lock-delay to determine profile in use, needed for remaining tests

l_kfd2="/etc/dconf/db/$(grep -Psril '^\h*lock-delay\h*=\h*uint32\h+\d+\b' /etc/dconf/db/*/ | awk -F'/'
'{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked

if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked

if grep -Prilq '^\h*\/org\/gnome\/desktop\/session\/idle-delay\b' "$l_kfd"; then

echo " - \"idle-delay\" is locked in \"$(grep -Pril '^\h*\/org\/gnome\/desktop\/session\/idle-delay\b'
"$l_kfd")\""

else

echo "creating entry to lock \"idle-delay\""

[ ! -d "$l_kfd"/locks ] && echo "creating directory $l_kfd/locks" && mkdir "$l_kfd"/locks

{

echo -e '\n# Lock desktop screensaver idle-delay setting'

echo '/org/gnome/desktop/session/idle-delay'

} >> "$l_kfd"/locks/00-screensaver

fi

else

echo -e " - \"idle-delay\" is not set so it can not be locked\n - Please follow Recommendation \"Ensure
GDM screen locks when the user is idle\" and follow this Recommendation again"

fi

if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist, options can't be locked

if grep -Prilq '^\h*\/org\/gnome\/desktop\/screensaver\/lock-delay\b' "$l_kfd2"; then

echo " - \"lock-delay\" is locked in \"$(grep -Pril '^\h*\/org\/gnome\/desktop\/screensaver\/lock-
delay\b' "$l_kfd2")\""

else

echo "creating entry to lock \"lock-delay\""

[ ! -d "$l_kfd2"/locks ] && echo "creating directory $l_kfd2/locks" && mkdir "$l_kfd2"/locks

{

echo -e '\n# Lock desktop screensaver lock-delay setting'

echo '/org/gnome/desktop/screensaver/lock-delay'

} >> "$l_kfd2"/locks/00-screensaver

fi

else

echo -e " - \"lock-delay\" is not set so it can not be locked\n - Please follow Recommendation \"Ensure
GDM screen locks when the user is idle\" and follow this Recommendation again"

fi

else
```

```
echo -e " - GNOME Desktop Manager package is not installed on the system\n - Recommendation is not
applicable"

fi

}
```

Run the following command to update the system databases:

```
# dconf update
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://help.gnome.org/admin/system-admin-guide/stable/desktop-lockscreen.html.en
- **URL:** https://help.gnome.org/admin/system-admin-guide/stable/dconf-lockdown.html.en
- **URL:** NIST SP 800-53 Rev. 5: CM-11

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

1.8.6 Ensure GDM automatic mounting of removable media is disabled

Pass

Description:

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

Rationale:

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

Remediation:

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

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



{

l_pkgoutput="" l_output="" l_output2=""

l_gpname="local" # Set to desired dconf profile name (defaule is local)

# Check if GNOME Desktop Manager is installed. If package isn't installed, recommendation is Not
Applicable\n

# determine system's package manager

if command -v dpkg-query > /dev/null 2>&1; then

l_pq="dpkg-query -W"

elif command -v rpm > /dev/null 2>&1; then

l_pq="rpm -q"

fi

# Check if GDM is installed

l_pcl="gdm gdm3" # Space seporated list of packages to check
```

```
for l_pn in $l_pcl; do

$l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists on the
system\n - checking configuration"

done

echo -e "$l_packageout"

# Check configuration (If applicable)

if [ -n "$l_pkgoutput" ]; then

echo -e "$l_pkgoutput"

# Look for existing settings and set variables if they exist

l_kfile="$(grep -Prils -- '^\h*automount\b' /etc/dconf/db/*.d)"

l_kfile2="$(grep -Prils -- '^\h*automount-open\b' /etc/dconf/db/*.d)"

# Set profile name based on dconf db directory ({PROFILE_NAME}.d)

if [ -f "$l_kfile" ]; then

l_gpname="$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<< "$l_kfile")"

echo " - updating dconf profile name to \"$l_gpname\""

elif [ -f "$l_kfile2" ]; then

l_gpname="$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<< "$l_kfile2")"

echo " - updating dconf profile name to \"$l_gpname\""

fi

# check for consistency (Clean up configuration if needed)

if [ -f "$l_kfile" ] && [ "$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<< "$l_kfile")" !=
"$l_gpname" ]; then

sed -ri "/^\s*automount\s*=/s/^/# /" "$l_kfile"

l_kfile="/etc/dconf/db/$l_gpname.d/00-media-automount"

fi

if [ -f "$l_kfile2" ] && [ "$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<< "$l_kfile2")" !=
"$l_gpname" ]; then

sed -ri "/^\s*automount-open\s*=/s/^/# /" "$l_kfile2"

fi

[ -z "$l_kfile" ] && l_kfile="/etc/dconf/db/$l_gpname.d/00-media-automount"

# Check if profile file exists

if grep -Pq -- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*; then

echo -e "\n - dconf database profile exists in: \"$(grep -Pl -- "^\h*system-db:$l_gpname\b"
/etc/dconf/profile/*)\""

else

[ ! -f "/etc/dconf/profile/user" ] && l_gpfile="/etc/dconf/profile/user" ||
l_gpfile="/etc/dconf/profile/user2"

echo -e " - creating dconf database profile"

{

echo -e "\nuser-db:user"

echo "system-db:$l_gpname"

} >> "$l_gpfile"

fi

# create dconf directory if it doesn't exists

l_gpdir="/etc/dconf/db/$l_gpname.d"

if [ -d "$l_gpdir" ]; then
```

```
echo " - The dconf database directory \"$l_gpdir\" exists"

else

echo " - creating dconf database directory \"$l_gpdir\""

mkdir "$l_gpdir"

fi

# check automount-open setting

if grep -Pqs -- '^\h*automount-open\h*=\h*false\b' "$l_kfile"; then

echo " - \"automount-open\" is set to false in: \"$l_kfile\""

else

echo " - creating \"automount-open\" entry in \"$l_kfile\""

! grep -Psq -- '\^\h*\[org\/gnome\/desktop\/media-handling\]\b' "$l_kfile" && echo
'[org/gnome/desktop/media-handling]' >> "$l_kfile"

sed -ri '/^\s*\[org\/gnome\/desktop\/media-handling\]/a \\nautomount-open=false' "$l_kfile"

fi

# check automount setting

if grep -Pqs -- '^\h*automount\h*=\h*false\b' "$l_kfile"; then

echo " - \"automount\" is set to false in: \"$l_kfile\""

else

echo " - creating \"automount\" entry in \"$l_kfile\""

! grep -Psq -- '\^\h*\[org\/gnome\/desktop\/media-handling\]\b' "$l_kfile" && echo
'[org/gnome/desktop/media-handling]' >> "$l_kfile"

sed -ri '/^\s*\[org\/gnome\/desktop\/media-handling\]/a \\nautomount=false' "$l_kfile"

fi

else

echo -e "\n - GNOME Desktop Manager package is not installed on the system\n - Recommendation is not
applicable"

fi

# update dconf database

dconf update

}
```

OR

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

```
# apt purge gdm3
```

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.

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://access.redhat.com/solutions/20107
- **URL:** NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More >

Back to Summary

1.8.7 Ensure GDM disabling automatic mounting of removable media is not overridden

Pass

Description:

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

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

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

Example Lock File:

```
# Lock desktop screensaver settings

/org/gnome/desktop/media-handling/automount

/org/gnome/desktop/media-handling/automount-open
```

Rationale:

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

Remediation:

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

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



{

# Check if GNMOE Desktop Manager is installed. If package isn't installed, recommendation is Not
Applicable\n

# determine system's package manager

l_pkgoutput=""

if command -v dpkg-query > /dev/null 2>&1; then

l_pq="dpkg-query -W"

elif command -v rpm > /dev/null 2>&1; then

l_pq="rpm -q"

fi

# Check if GDM is installed

l_pcl="gdm gdm3" # Space seporated list of packages to check

for l_pn in $l_pcl; do

$l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="y" && echo -e "\n - Package: \"$l_pn\" exists on the
system\n - remediating configuration if needed"

done

# Check configuration (If applicable)

if [ -n "$l_pkgoutput" ]; then

# Look for automount to determine profile in use, needed for remaining tests

l_kfd="/etc/dconf/db/$(grep -Psril '^\h*automount\b' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-
1),a,".");print a[1]}').d" #set directory of key file to be locked

# Look for automount-open to determine profile in use, needed for remaining tests
```

```
l_kfd2="/etc/dconf/db/$(grep -Psril '^\h*automount-open\b' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-
1),a,".");print a[1]}').d" #set directory of key file to be locked

if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked

if grep -Priq '^\h*\/org/gnome\/desktop\/media-handling\/automount\b' "$l_kfd"; then

echo " - \"automount\" is locked in \"$(grep -Pril '^\h*\/org/gnome\/desktop\/media-
handling\/automount\b' "$l_kfd")\""

else

echo " - creating entry to lock \"automount\""

[ ! -d "$l_kfd"/locks ] && echo "creating directory $l_kfd/locks" && mkdir "$l_kfd"/locks

{

echo -e '\n# Lock desktop media-handling automount setting'

echo '/org/gnome/desktop/media-handling/automount'

} >> "$l_kfd"/locks/00-media-automount

fi

else

echo -e " - \"automount\" is not set so it can not be locked\n - Please follow Recommendation \"Ensure
GDM automatic mounting of removable media is disabled\" and follow this Recommendation again"

fi

if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist, options can't be locked

if grep -Priq '^\h*\/org/gnome\/desktop\/media-handling\/automount-open\b' "$l_kfd2"; then

echo " - \"automount-open\" is locked in \"$(grep -Pril '^\h*\/org/gnome\/desktop\/media-
handling\/automount-open\b' "$l_kfd2")\""

else

echo " - creating entry to lock \"automount-open\""

[ ! -d "$l_kfd2"/locks ] && echo "creating directory $l_kfd2/locks" && mkdir "$l_kfd2"/locks

{

echo -e '\n# Lock desktop media-handling automount-open setting'

echo '/org/gnome/desktop/media-handling/automount-open'

} >> "$l_kfd2"/locks/00-media-automount

fi

else

echo -e " - \"automount-open\" is not set so it can not be locked\n - Please follow Recommendation
\"Ensure GDM automatic mounting of removable media is disabled\" and follow this Recommendation again"

fi

# update dconf database

dconf update

else

echo -e " - GNOME Desktop Manager package is not installed on the system\n - Recommendation is not
applicable"

fi

}
```

Impact:

The use of portable hard drives is very common for workstation users

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://help.gnome.org/admin/system-admin-guide/stable/dconf-lockdown.html.en
- **URL:** NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

Back to Summary

1.8.8 Ensure GDM autorun-never is enabled

Pass

Description:

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

Rationale:

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

Remediation:

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

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



{

l_pkgoutput="" l_output="" l_output2=""

l_gpname="local" # Set to desired dconf profile name (default is local)

# Check if GNOME Desktop Manager is installed. If package isn't installed, recommendation is Not
Applicable\n

# determine system's package manager

if command -v dpkg-query > /dev/null 2>&1; then

l_pq="dpkg-query -W"

elif command -v rpm > /dev/null 2>&1; then

l_pq="rpm -q"

fi

# Check if GDM is installed

l_pcl="gdm gdm3" # Space separated list of packages to check

for l_pn in $l_pcl; do

$l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists on the
system\n - checking configuration"

done

echo -e "$l_pkgoutput"

# Check configuration (If applicable)

if [ -n "$l_pkgoutput" ]; then

echo -e "$l_pkgoutput"

# Look for existing settings and set variables if they exist

l_kfile="$(grep -Prils -- '^\h*autorun-never\b' /etc/dconf/db/*.d)"

# Set profile name based on dconf db directory ({PROFILE_NAME}.d)

if [ -f "$l_kfile" ]; then

l_gpname="$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<< "$l_kfile")"

echo " - updating dconf profile name to \"$l_gpname\""

fi

[ ! -f "$l_kfile" ] && l_kfile="/etc/dconf/db/$l_gpname.d/00-media-autorun"

# Check if profile file exists
```

```
if grep -Pq -- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*; then

echo -e "\n - dconf database profile exists in: \"$(grep -Pl -- "^\h*system-db:$l_gpname\b"
/etc/dconf/profile/*)\""

else

[ ! -f "/etc/dconf/profile/user" ] && l_gpfile="/etc/dconf/profile/user" ||
l_gpfile="/etc/dconf/profile/user2"

echo -e " - creating dconf database profile"

{

echo -e "\nuser-db:user"

echo "system-db:$l_gpname"

} >> "$l_gpfile"

fi

# create dconf directory if it doesn't exists

l_gpdir="/etc/dconf/db/$l_gpname.d"

if [ -d "$l_gpdir" ]; then

echo " - The dconf database directory \"$l_gpdir\" exists"

else

echo " - creating dconf database directory \"$l_gpdir\""

mkdir "$l_gpdir"

fi

# check autorun-never setting

if grep -Pqs -- '^\h*autorun-never\h*=\h*true\b' "$l_kfile"; then

echo " - \"autorun-never\" is set to true in: \"$l_kfile\""

else

echo " - creating or updating \"autorun-never\" entry in \"$l_kfile\""

if grep -Psq -- '^\h*autorun-never' "$l_kfile"; then

sed -ri 's/(^\s*autorun-never\s*=\s*)(\S+)(\s*.*)$/\1true \3/' "$l_kfile"

else

! grep -Psq -- '\^\h*\[org\/gnome\/desktop\/media-handling\]\b' "$l_kfile" && echo
'[org/gnome/desktop/media-handling]' >> "$l_kfile"

sed -ri '/^\s*\[org\/gnome\/desktop\/media-handling\]/a \\nautorun-never=true' "$l_kfile"

fi

fi

else

echo -e "\n - GNOME Desktop Manager package is not installed on the system\n - Recommendation is not
applicable"

fi

# update dconf database

dconf update

}
```

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
  >

Back to Summary

1.8.9 Ensure GDM autorun-never is not overridden

Pass

Description:

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

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

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

Example Lock File:

```
# Lock desktop media-handling settings

/org/gnome/desktop/media-handling/autorun-never
```

Rationale:

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

Remediation:

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

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



{

# Check if GNOME Desktop Manager is installed. If package isn't installed, recommendation is Not
Applicable\n

# determine system's package manager

l_pkgoutput=""

if command -v dpkg-query > /dev/null 2>&1; then

l_pq="dpkg-query -W"

elif command -v rpm > /dev/null 2>&1; then

l_pq="rpm -q"

fi

# Check if GDM is installed

l_pcl="gdm gdm3" # Space separated list of packages to check

for l_pn in $l_pcl; do

$l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="y" && echo -e "\n - Package: \"$l_pn\" exists on the
system\n - remediating configuration if needed"

done

# Check configuration (If applicable)

if [ -n "$l_pkgoutput" ]; then

# Look for autorun to determine profile in use, needed for remaining tests

l_kfd="/etc/dconf/db/$(grep -Psril '^\h*autorun-never\b' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-
1),a,".");print a[1]}').d" #set directory of key file to be locked
```

```
if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked

if grep -Prisq '^\h*\/org/gnome\/desktop\/media-handling\/autorun-never\b' "$l_kfd"; then

echo " - \"autorun-never\" is locked in \"$(grep -Pril '^\h*\/org/gnome\/desktop\/media-
handling\/autorun-never\b' "$l_kfd")\""

else

echo " - creating entry to lock \"autorun-never\""

[ ! -d "$l_kfd"/locks ] && echo "creating directory $l_kfd/locks" && mkdir "$l_kfd"/locks

{

echo -e '\n# Lock desktop media-handling autorun-never setting'

echo '/org/gnome/desktop/media-handling/autorun-never'

} >> "$l_kfd"/locks/00-media-autorun

fi

else

echo -e " - \"autorun-never\" is not set so it can not be locked\n - Please follow Recommendation
\"Ensure GDM autorun-never is enabled\" and follow this Recommendation again"

fi

# update dconf database

dconf update

else

echo -e " - GNOME Desktop Manager package is not installed on the system\n - Recommendation is not
applicable"

fi

}
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
  >

Back to Summary

1.8.10 Ensure XDCMP is not enabled

Pass

Description:

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

Rationale:

XDMCP is inherently insecure.

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

Remediation:

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

```
Enable=true
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SI-4

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2 Services

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

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

2.1 Configure Time Synchronization

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

Note:

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

2.1.1 Ensure time synchronization is in use

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

2.1.1.1 Ensure a single time synchronization daemon is in use

Pass

Description:

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

Note:

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

Rationale:

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

Remediation:

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

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

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

1. `chrony`

Run the following command to install `chrony` :

```
# apt install chrony
```

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

```
# systemctl stop systemd-timesyncd.service



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

Run the following command to remove the ntp package:

```
# apt purge ntp
```

NOTE:

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

2. `systemd-timesyncd`

Run the following command to remove the chrony package:

```
# apt purge chrony
```

Run the following command to remove the ntp package:

```
# apt purge ntp
```

NOTE:

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

3. `ntp`

Run the following command to install `ntp` :

```
# apt install ntp
```

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

```
# systemctl stop systemd-timesyncd.service



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

Run the following command to remove the chrony package:

```
# apt purge chrony
```

NOTE:

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-3, AU-12

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

2.1.2 Configure chrony

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

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

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

Note:

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

2.1.2.1 Ensure chrony is configured with authorized timeserver

Manual

Description:

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

Rationale:

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

Remediation:

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

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

Examples:

`pool` *directive:*

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

`server` *directive:*

```
server time-a-g.nist.gov iburst

server 132.163.97.3 iburst

server time-d-b.nist.gov iburst
```

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

```
# systemctl restart chronyd


- OR if sources are in a .sources file -


# chronyc reload sources
```

OR

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

```
# apt purge chrony
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** chrony.conf(5) Manual Page
- **URL:** https://tf.nist.gov/tf-cgi/servers.cgi
- **URL:** NIST SP 800-53 Rev. 5: AU-3, AU-12

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

2.1.2.2 Ensure chrony is running as user _chrony

Pass

Description:

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

Rationale:

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

Remediation:

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

```
user _chrony
```

OR

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

```
# apt purge chrony
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-8

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

2.1.2.3 Ensure chrony is enabled and running

Pass

Description:

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

Rationale:

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

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

Remediation:

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

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

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

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

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

OR

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

```
# apt purge chrony
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-8

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

2.1.3 Configure systemd-timesyncd

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

The default configuration is set during compilation, so configuration is only needed when it is necessary to deviate from those defaults. Initially, the main configuration file in /etc/systemd/ contains commented out entries showing the defaults as

a guide to the administrator. Local overrides can be created by editing this file or by creating drop-ins, as described below. Using drop-ins for local configuration is recommended over modifications to the main configuration file.

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

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

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

Note:

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

2.1.3.1 Ensure systemd-timesyncd configured with authorized timeserver

Fail

Description:

`NTP=`

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

`FallbackNTP=`

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

Rationale:

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

Remediation:

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

Example:

```
[Time]

NTP=time.nist.gov # Uses the generic name for NIST's time servers

-AND/OR-

FallbackNTP=time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov # Space separated list of NIST time
servers
```

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

Example script:

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

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



{

l_ntp_ts="time.nist.gov"
```

```
l_ntp_fb="time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov"

l_conf_file="/etc/systemd/timesyncd.conf"

if ! grep -Ph '^\h*NTP=\H+' "$l_conf_file"; then

! grep -Pqs '^\h*\[Time\]' "$l_conf_file" && echo "[Time]" >> "$l_conf_file"

echo "NTP=$l_ntp_ts" >> "$l_conf_file"

fi

if ! grep -Ph '^\h*FallbackNTP=\H+' "$l_conf_file"; then

! grep -Pqs '^\h*\[Time\]' "$l_conf_file" && echo "[Time]" >> "$l_conf_file"

echo "FallbackNTP=$l_ntp_fb" >> "$l_conf_file"

fi

}
```

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

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

-OR-

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://www.freedesktop.org/software/systemd/man/timesyncd.conf.html
- **URL:** https://tf.nist.gov/tf-cgi/servers.cgi
- **URL:** NIST SP 800-53 Rev. 5: AU-7, AU-8

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

2.1.3.2 Ensure systemd-timesyncd is enabled and running

Manual

Description:

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network

Rationale:

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

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

Remediation:

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

Run the following command to unmask `systemd-timesyncd.service`:

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

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

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

OR

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-7, AU-8

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

2.1.4 Configure ntp

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

Note:

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

2.1.4.1 Ensure ntp access control is configured

Pass

Description:

`ntp` Access Control Commands:

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

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

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

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

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

One or more of the following flags may be specified:

- `kod` - If this flag is set when an access violation occurs, a kiss-o'-death (KoD) packet is sent. KoD packets are rate limited to no more than one per second. If another KoD packet occurs within one second after the last one, the packet is dropped.

- `limited` - Deny service if the packet spacing violates the lower limits specified in the discard command. A history of clients is kept using the monitoring capability of `ntpd` . Thus, monitoring is always active as long as there is a restriction entry with the limited flag.
- `lowpriotrap` - Declare traps set by matching hosts to be low priority. The number of traps a server can maintain is limited (the current limit is 3). Traps are usually assigned on a first come, first served basis, with later trap requestors being denied service. This flag modifies the assignment algorithm by allowing low priority traps to be overridden by later requests for normal priority traps.
- `noepeer` - Deny ephemeral peer requests, even if they come from an authenticated source. Note that the ability to use a symmetric key for authentication may be restricted to one or more IPs or subnets via the third field of the ntp.keys file. This restriction is not enabled by default, to maintain backward compatibility. Expect noepeer to become the default in `ntp-4.4` .
- `nomodify` - Deny `ntpq` and `ntpdc` queries which attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.
- `noquery` - Deny `ntpq` and `ntpdc` queries. Time service is not affected.
- `nopeer` - Deny unauthenticated packets which would result in mobilizing a new association. This includes broadcast and symmetric active packets when a configured association does not exist. It also includes pool associations, so if you want to use servers from a pool directive and also want to use `nopeer` by default, you'll want a restrict source ... line as well that does not include the `nopeer` directive.
- `noserve` - Deny all packets except `ntpq` and `ntpdc` queries.
- `notrap` - Decline to provide mode 6 control message trap service to matching hosts. The trap service is a subsystem of the `ntpq` control message protocol which is intended for use by remote event logging programs.
- `notrust` - Deny service unless the packet is cryptographically authenticated.
- `ntpport` - This is actually a match algorithm modifier, rather than a restriction flag. Its presence causes the restriction entry to be matched only if the source port in the packet is the standard NTP UDP port (123). Both `ntpport` and `non-ntpport` may be specified. The `ntpport` is considered more specific and is sorted later in the list.

Rationale:

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

Remediation:

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

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

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

OR

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

```
# apt purge ntp
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** http://www.ntp.org/
- **URL:** ntp.conf(5)
- **URL:** ntpd(8)
- **URL:** NIST SP 800-53 Rev. 5: AU-8

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

2.1.4.2 Ensure ntp is configured with authorized timeserver

Manual

Description:

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

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

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

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

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

Rationale:

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

Remediation:

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

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

Examples:

`pool` *mode:*

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

`server` *mode:*

```
server time-a-g.nist.gov iburst

server 132.163.97.3 iburst

server time-d-b.nist.gov iburst
```

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

```
# systemctl restart ntp
```

OR

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

```
# apt purge ntp
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** http://www.ntp.org/
- **URL:** https://tf.nist.gov/tf-cgi/servers.cgi
- **URL:** ntp.conf(5)
- **URL:** ntpd(8)
- **URL:** NIST SP 800-53 Rev. 5: AU-8

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

2.1.4.3 Ensure ntp is running as user ntp

Pass

Description:

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

Note:

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

Rationale:

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

Remediation:

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

```
RUNASUSER=ntp
```

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

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

OR

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

```
# apt purge ntp
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** http://www.ntp.org/
- **URL:** NIST SP 800-53 Rev. 5: AU-8

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

2.1.4.4 Ensure ntp is enabled and running

Pass

Description:

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

Rationale:

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

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

Remediation:

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

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

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

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

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

OR

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

```
# apt purge ntp
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-8

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

2.2 Special Purpose Services

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

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

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

2.2.2 Ensure Avahi Server is not installed

Pass

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.

Remediation:

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

```
# systemctl stop avahi-daaemon.service

# systemctl stop avahi-daemon.socket

# apt purge avahi-daemon
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SI-4

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.3 Ensure CUPS is not installed

Pass

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.

Remediation:

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

```
# apt purge cups
```

Impact:

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** More detailed documentation on CUPS is available at the project homepage at http://www.cups.org.
- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.4 Ensure DHCP Server is not installed

Pass

Description:

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

Rationale:

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

Remediation:

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.5 Ensure LDAP server is not installed

Pass

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.

Remediation:

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

```
# apt purge slapd
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.6 Ensure NFS is not installed

Pass

Description:

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

Rationale:

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

Remediation:

Run the following command to remove `nfs` :

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.7 Ensure DNS Server is not installed

Pass

Description:

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

Rationale:

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

Remediation:

Run the following commands to disable `DNS server` :

```
# apt purge bind9
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.8 Ensure FTP Server is not installed

Pass

Description:

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

Rationale:

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

Remediation:

Run the following command to remove `vsftpd` :

```
# apt purge vsftpd
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.9 Ensure HTTP server is not installed

Fail

Description:

HTTP or web servers provide the ability to host web site content.

Rationale:

Unless there is a need to run the system as a web server, it is recommended that the package be deleted to reduce the potential attack surface.

Remediation:

Run the following command to remove `apache2` :

```
# apt purge apache2
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.10 Ensure IMAP and POP3 server are not installed

Pass

Description:

`dovecot-imapd` and `dovecot-pop3d` are an open source IMAP and POP3 server for Linux based systems.

Rationale:

Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the package be removed to reduce the potential attack surface.

Remediation:

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.11 Ensure Samba is not installed

Pass

Description:

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Server Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems.

Rationale:

If there is no need to mount directories and file systems to Windows systems, then this service should be deleted to reduce the potential attack surface.

Remediation:

Run the following command to remove `samba` :

```
# apt purge samba
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.12 Ensure HTTP Proxy Server is not installed

Pass

Description:

Squid is a standard proxy server used in many distributions and environments.

Rationale:

If there is no need for a proxy server, it is recommended that the squid proxy be deleted to reduce the potential attack surface.

Remediation:

Run the following command to remove `squid` :

```
# apt purge squid
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.13 Ensure SNMP Server is not installed

Pass

Description:

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

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

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

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

Rationale:

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

Note: If SNMP is required:

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

Remediation:

Run the following command to remove `snmpd` :

```
# apt purge snmpd
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.14 Ensure NIS Server is not installed

Pass

Description:

The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files.

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed and other, more secure services be used

Remediation:

Run the following command to remove `nis` :

```
# apt purge nis
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.15 Ensure dnsmasq is not installed

Pass

Description:

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

Rationale:

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

Remediation:

Run the following command to remove `dnsmasq` :

```
# apt purge dnsmasq
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.2.16 Ensure mail transfer agent is configured for local-only mode

Pass

Description:

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.

Rationale:

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

Note:

- This recommendation is designed around the postfix mail server.
- Depending on your environment you may have an alternative MTA installed such as exim4. If this is the case consult the documentation for your installed MTA to configure the recommended state.

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
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More

>

Back to Summary

2.2.17 Ensure rsync service is either not installed or is masked

Pass

Description:

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

Rationale:

The `rsync` service presents a security risk as the `rsync protocol` is unencrypted. The `rsync` package should be removed or if required for dependencies, the `rsync` service should be stopped and masked to reduce the attack area of the system.

Remediation:

Run the following command to remove `rsync` :

```
# apt purge rsync
```

-- OR --

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

```
# systemctl stop rsync


# systemctl mask rsync
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

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.

2.3.1 Ensure NIS Client is not installed

Pass

Description:

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client was used to bind a machine to an NIS server and receive the distributed configuration files.

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight

Directory Access Protocol (LDAP). It is recommended that the service be removed.

Remediation:

Uninstall `nis` :

```
# apt purge nis
```

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.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7, CM-11

CIS Controls V7.0:

- **Control 2: Inventory and Control of Software Assets:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.3.2 Ensure rsh client is not installed

Pass

Description:

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

Rationale:

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

Remediation:

Uninstall `rsh` :

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

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.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.3.3 Ensure talk client is not installed

Pass

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.

Remediation:

Uninstall `talk` :

```
# apt purge talk
```

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.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.3.4 Ensure telnet client is not installed

Fail

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.

Remediation:

Uninstall `telnet` :

```
# apt purge telnet
```

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.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7, CM-11

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.3.5 Ensure LDAP client is not installed

Pass

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.

Remediation:

Uninstall `ldap-utils` :

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

Impact:

Removing the LDAP client will prevent or inhibit using LDAP for authentication in your environment.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.3.6 Ensure RPC is not installed

Pass

Description:

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

Rationale:

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

Remediation:

Run the following command to remove `rpcbind` :

```
# apt purge rpcbind
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.4 Ensure nonessential services are removed or masked

Manual

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.

Remediation:

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

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

***OR** If required packages have a dependency:*

Run the following commands to stop and mask the service:

```
# systemctl stop <service_name>.socket

# systemctl stop <service_name>.service

# systemctl mask <service_name>.socket

# systemctl mask <service_name>.service
```

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3 Network Configuration

This section provides guidance on for securing the network configuration of the system through kernel parameters, access list control, and firewall settings.

Note:

- sysctl settings are defined through files in `/usr/lib/sysctl.d/` , `/run/sysctl.d/` , and `/etc/sysctl.d/` .
- Files must have the " `.conf` " extension.
- Vendors settings live in `/usr/lib/sysctl.d/`
- To override a whole file, create a new file with the same name in `/etc/sysctl.d/` and put new settings there.
- To override only specific settings, add a file with a lexically later name in `/etc/sysctl.d/` and put new settings there.
- The paths where sysctl preload files usually exist
  - `/run/sysctl.d/*.conf`
  - `/etc/sysctl.d/*.conf`
  - `/usr/local/lib/sysctl.d/*.conf`
  - `/usr/lib/sysctl.d/*.conf`
  - `/lib/sysctl.d/*.conf`
  - `/etc/sysctl.conf`
- On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`
  - The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
  - This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

3.1 Disable unused network protocols and devices

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

The Linux kernel modules support several network protocols that are not commonly used. If these protocols are not needed, it is recommended that they be disabled in the kernel.

Note: This should not be considered a comprehensive list of uncommon network protocols, you may wish to consider additions to those listed here for your environment.

3.1.1 Ensure IPv6 status is identified

Manual

Description:

Internet Protocol Version 6 (IPv6) is the most recent version of Internet Protocol (IP). It's designed to supply IP addressing and additional security to support the predicted growth of connected devices. IPv6 is based on 128-bit addressing and can support 340 undecillion addresses, which is 340 followed by 36 zeroes.

Features of IPv6

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

Rationale:

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

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

Note: It is recommended that IPv6 be enabled and configured unless this is against local site policy

Remediation:

Enable or disable IPv6 in accordance with system requirements and local site policy

Impact:

IETF RFC 4038 recommends that applications are built with an assumption of dual stack.

When enabled, IPv6 will require additional configuration to reduce risk to the system.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.1.2 Ensure wireless interfaces are disabled

Pass

Description:

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

Rationale:

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

Remediation:

Run the following script to disable any wireless interfaces:

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


{

module_fix()

{

if ! modprobe -n -v "$l_mname" | grep -P -- '^\h*install \/bin\/(true|false)'; then

echo -e " - setting module: \"$l_mname\" to be un-loadable"

echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mname".conf

fi

if lsmod | grep "$l_mname" > /dev/null 2>&1; then

echo -e " - unloading module \"$l_mname\""

modprobe -r "$l_mname"

fi

if ! grep -Pq -- "^\h*blacklist\h+$l_mname\b" /etc/modprobe.d/*; then

echo -e " - deny listing \"$l_mname\""

echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mname".conf

fi

}

if [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then

l_dname=$(for driverdir in $(find /sys/class/net/*/ -type d -name wireless | xargs -0 dirname); do
basename "$(readlink -f "$driverdir"/device/driver/module)";done | sort -u)

for l_mname in $l_dname; do

module_fix
```

```
done

fi

}
```

Impact:

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 15: Wireless Access Control:** -- More
- **Control 15: Wireless Access Control:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

3.1.3 Ensure bluetooth is disabled

Pass

Description:

Bluetooth is a short-range wireless technology standard that is used for exchanging data between devices over short distances. It employs UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz. It is mainly used as an alternative to wire connections.

Rationale:

An attacker may be able to find a way to access or corrupt your data. One example of this type of activity is `bluesnarfing` , which refers to attackers using a Bluetooth connection to steal information off of your Bluetooth device. Also, viruses or other malicious code can take advantage of Bluetooth technology to infect other devices. If you are infected, your data may be corrupted, compromised, stolen, or lost.

Remediation:

Run the following commands to stop and mask the Bluetooth service

```
# systemctl stop bluetooth.service

# systemctl mask bluetooth.service
```

Note: A reboot may be required

Impact:

Many personal electronic devices (PEDs) use Bluetooth technology. For example, you may be able to operate your computer with a wireless keyboard. Disabling Bluetooth will prevent these devices from connecting to the system.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://www.cisa.gov/tips/st05-015
- **URL:** NIST SP 800-53 Rev. 5: CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.2 Network Parameters (Host Only)

The following network parameters are intended for use if the system is to act as a host only. A system is considered host only if the system has a single interface, or has multiple interfaces but will not be configured as a router.

Note:

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

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

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

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

3.2.1 Ensure packet redirect sending is disabled

Fail

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.

Remediation:

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

- `net.ipv4.conf.all.send_redirects = 0`
- `net.ipv4.conf.default.send_redirects = 0`

Example:

```
# printf "

net.ipv4.conf.all.send_redirects = 0

net.ipv4.conf.default.send_redirects = 0

" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {

sysctl -w net.ipv4.conf.all.send_redirects=0

sysctl -w net.ipv4.conf.default.send_redirects=0

sysctl -w net.ipv4.route.flush=1

}
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.2.2 Ensure IP forwarding is disabled

Fail

Description:

The `net.ipv4.ip_forward` and `net.ipv6.conf.all.forwarding` flags are used to tell the system whether it can forward packets or not.

Rationale:

Setting `net.ipv4.ip_forward` and `net.ipv6.conf.all.forwarding` to `0` ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Remediation:

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

- `net.ipv4.ip_forward = 0`

Example:

```
# printf "

net.ipv4.ip_forward = 0

" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {

sysctl -w net.ipv4.ip_forward=0

sysctl -w net.ipv4.route.flush=1

}
```

-IF- IPv6 is enabled on the system:

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

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

Example:

```
# printf "

net.ipv6.conf.all.forwarding = 0

" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
```

```
sysctl -w net.ipv6.conf.all.forwarding=0

sysctl -w net.ipv6.route.flush=1

}
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.3 Network Parameters (Host and Router)

The following network parameters are intended for use on both host only and router systems. A system acts as a router if it has at least two interfaces and is configured to perform routing functions.

Note:

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

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

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

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

3.3.1 Ensure source routed packets are not accepted

Fail

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.

Remediation:

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

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

Example:

```
# printf "

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {

sysctl -w net.ipv4.conf.all.accept_source_route=0

sysctl -w net.ipv4.conf.default.accept_source_route=0

sysctl -w net.ipv4.route.flush=1

}
```

-IF- IPv6 is enabled on the system:

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

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

Example:

```
# printf "

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {

sysctl -w net.ipv6.conf.all.accept_source_route=0

sysctl -w net.ipv6.conf.default.accept_source_route=0

sysctl -w net.ipv6.route.flush=1

}
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.3.2 Ensure ICMP redirects are not accepted

Fail

Description:

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables.

Rationale:

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting `net.ipv4.conf.all.accept_redirects` , `net.ipv4.conf.default.accept_redirects` , `net.ipv6.conf.all.accept_redirects` , and `net.ipv6.conf.default.accept_redirects` to `0` , the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Remediation:

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

- `net.ipv4.conf.all.accept_redirects = 0`
- `net.ipv4.conf.default.accept_redirects = 0`

Example:

```
# printf "

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {

sysctl -w net.ipv4.conf.all.accept_redirects=0

sysctl -w net.ipv4.conf.default.accept_redirects=0

sysctl -w net.ipv4.route.flush=1

}
```

-IF- IPv6 is enabled on the system:

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

- `net.ipv6.conf.all.accept_redirects = 0`
- `net.ipv6.conf.default.accept_redirects = 0`

Example:

```
# printf "

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {

sysctl -w net.ipv6.conf.all.accept_redirects=0

sysctl -w net.ipv6.conf.default.accept_redirects=0

sysctl -w net.ipv6.route.flush=1

}
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.3.3 Ensure secure ICMP redirects are not accepted

Fail

Description:

Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure.

Rationale:

It is still possible for even known gateways to be compromised. Setting `net.ipv4.conf.all.secure_redirects` and `net.ipv4.conf.default.secure_redirects` to `0` protects the system from routing table updates by possibly compromised known gateways.

Remediation:

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

- `net.ipv4.conf.all.secure_redirects = 0`
- `net.ipv4.conf.default.secure_redirects = 0`

Example:

```
# printf "

net.ipv4.conf.all.secure_redirects = 0

net.ipv4.conf.default.secure_redirects = 0

" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following commands to set the active kernel parameters:

```
# {

sysctl -w net.ipv4.conf.all.secure_redirects=0

sysctl -w net.ipv4.conf.default.secure_redirects=0

sysctl -w net.ipv4.route.flush=1

}
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.3.4 Ensure suspicious packets are logged

Fail

Description:

When enabled, this feature logs packets with un-routable source addresses to the kernel log.

Rationale:

Setting `net.ipv4.conf.all.log_martians` and `net.ipv4.conf.default.log_martians to 1` enables this feature. Logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Remediation:

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

- `net.ipv4.conf.all.log_martians = 1`
- `net.ipv4.conf.default.log_martians = 1`

Example:

```
# printf "

net.ipv4.conf.all.log_martians = 1

net.ipv4.conf.default.log_martians = 1

" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {

sysctl -w net.ipv4.conf.all.log_martians=1

sysctl -w net.ipv4.conf.default.log_martians=1

sysctl -w net.ipv4.route.flush=1

}
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-3

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

3.3.5 Ensure broadcast ICMP requests are ignored

Fail

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.

Remediation:

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

- `net.ipv4.icmp_echo_ignore_broadcasts = 1`

Example:

```
# printf "

net.ipv4.icmp_echo_ignore_broadcasts = 1

" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {

sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1

sysctl -w net.ipv4.route.flush=1

}
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.3.6 Ensure bogus ICMP responses are ignored

Fail

Description:

Setting `net.ipv4.icmp_ignore_bogus_error_responses` to `1` prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages.

Rationale:

Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

Remediation:

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

- `net.ipv4.icmp_ignore_bogus_error_responses = 1`

Example:

```
# printf "

net.ipv4.icmp_ignore_bogus_error_responses = 1

" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {

sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1

sysctl -w net.ipv4.route.flush=1

}
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.3.7 Ensure Reverse Path Filtering is enabled

Fail

Description:

Setting `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` to `1` forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the packet is dropped (and logged if `log_martians` is set).

Rationale:

Setting `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` to `1` is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Remediation:

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

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

Example:

```
# printf "

net.ipv4.conf.all.rp_filter = 1

net.ipv4.conf.default.rp_filter = 1

" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following commands to set the active kernel parameters:

```
# {

sysctl -w net.ipv4.conf.all.rp_filter=1

sysctl -w net.ipv4.conf.default.rp_filter=1

sysctl -w net.ipv4.route.flush=1

}
```

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

Impact:

If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.3.8 Ensure TCP SYN Cookies is enabled

Fail

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. Setting `net.ipv4.tcp_syncookies` to `1` enables SYN cookies, allowing the system to keep accepting valid connections, even if under a denial of service attack.

Remediation:

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

- `net.ipv4.tcp_syncookies = 1`

Example:

```
# printf "

net.ipv4.tcp_syncookies = 1

" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {

sysctl -w net.ipv4.tcp_syncookies=1
```

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

}
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.3.9 Ensure IPv6 router advertisements are not accepted

Fail

Description:

This setting disables the system's ability to accept IPv6 router advertisements.

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes. Setting `net.ipv6.conf.all.accept_ra` and `net.ipv6.conf.default.accept_ra` to `0` disables the system's ability to accept IPv6 router advertisements.

Remediation:

-IF- IPv6 is enabled on the system:

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

- `net.ipv6.conf.all.accept_ra = 0`
- `net.ipv6.conf.default.accept_ra = 0`

Example:

```
# printf "

net.ipv6.conf.all.accept_ra = 0

net.ipv6.conf.default.accept_ra = 0

" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {

sysctl -w net.ipv6.conf.all.accept_ra=0

sysctl -w net.ipv6.conf.default.accept_ra=0

sysctl -w net.ipv6.route.flush=1

}
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4 Firewall Configuration

A firewall is a set of rules. When a data packet moves into or out of a protected network space, its contents (in particular, information about its origin, target, and the protocol it plans to use) are tested against the firewall rules to see if it should be allowed through

To provide a Host Based Firewall, the Linux kernel includes support for:

- Netfilter - A set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack. Includes the ip_tables, ip6_tables, arp_tables, and ebtables kernel modules. These modules are some of the significant parts of the Netfilter hook system.
- nftables - A subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames. nftables is supposed to replace certain parts of Netfilter, while keeping and reusing most of it. nftables utilizes the building blocks of the Netfilter infrastructure, such as the existing hooks into the networking stack, connection tracking system, userspace queueing component, and logging subsystem. *Is available in Linux kernels 3.13 and newer* .

In order to configure firewall rules for Netfilter or nftables, a firewall utility needs to be installed. Guidance has been included for the following firewall utilities:

- UncomplicatedFirewall (ufw) - Provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the iptables backend. `ufw` supports both IPv4 and IPv6 networks
- nftables - Includes the nft utility for configuration of the nftables subsystem of the Linux kernel
- iptables - Includes the iptables, ip6tables, arptables and ebtables utilities for configuration Netfilter and the ip_tables, ip6_tables, arp_tables, and ebtables kernel modules.

Note:

- Only **one** method should be used to configure a firewall on the system. Use of more than one method could produce unexpected results
- This section is intended only to ensure the resulting firewall rules are in place, not how they are configured

3.4.1 Configure UncomplicatedFirewall

If nftables or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

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

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

Note:

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

3.4.1.1 Ensure ufw is installed

Fail

Description:

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

Rationale:

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

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

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

Remediation:

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

```
apt install ufw
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.1.2 Ensure iptables-persistent is not installed with ufw

Pass

Description:

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

Rationale:

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

Remediation:

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.1.3 Ensure ufw service is enabled

Fail

Description:

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

Note:

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

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

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

Rationale:

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

Remediation:

Run the following command to unmask the `ufw` daemon:

```
# systemctl unmask ufw.service
```

Run the following command to enable and start the `ufw` daemon:

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



active
```

Run the following command to enable ufw:

```
# ufw enable
```

Impact:

Changing firewall settings while connected over network can result in being locked out of the system.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** http://manpages.ubuntu.com/manpages/precise/en/man8/ufw.8.html
- **URL:** NIST SP 800-53 Rev. 5: SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.1.4 Ensure ufw loopback traffic is configured

Fail

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Remediation:

Run the following commands to implement the loopback rules:

```
# ufw allow in on lo

# ufw allow out on lo

# ufw deny in from 127.0.0.0/8

# ufw deny in from ::1
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.1.5 Ensure ufw outbound connections are configured

Manual

Description:

Configure the firewall rules for new outbound connections.

Note:

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

Rationale:

If rules are not in place for new outbound connections all packets will be dropped by the default policy preventing network usage.

Remediation:

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

```
# ufw allow out on all
```

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.1.6 Ensure ufw firewall rules exist for all open ports

Fail

Description:

Services and ports can be accepted or explicitly rejected.

Note:

- Changing firewall settings while connected over network can result in being locked out of the system
- The remediation command opens up the port to traffic from all sources. Consult ufw documentation and set any restrictions in compliance with site policy

Rationale:

To reduce the attack surface of a system, all services and ports should be blocked unless required.

- Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.
- Without a firewall rule configured for open ports, the default firewall policy will drop all packets to these ports.
- Required ports should have a firewall rule created to allow approved connections in accordance with local site policy.
- Unapproved ports should have an explicit deny rule created.

Remediation:

For each port identified in the audit which does not have a firewall rule, evaluate the service listening on the port and add a rule for accepting or denying inbound connections in accordance with local site policy:

Examples:

```
# ufw allow in <port>/<tcp or udp protocol>


# ufw deny in <port>/<tcp or udp protocol>
```

Note: Examples create rules for from any, to any. More specific rules should be concentered when allowing inbound traffic e.g only traffic from this network.

Example to allow traffic on port 443 using the tcp protocol from the 192.168.1.0 network:

```
ufw allow from 192.168.1.0/24 to any proto tcp port 443
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.1.7 Ensure ufw default deny firewall policy

Fail

Description:

A default deny policy on connections ensures that any unconfigured network usage will be rejected.

Note: Any port or protocol without a explicit allow before the default deny will be blocked

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Remediation:

Run the following commands to implement a default *deny* policy:

```
# ufw default deny incoming

# ufw default deny outgoing

# ufw default deny routed
```

Impact:

Any port and protocol not explicitly allowed will be blocked. The following rules should be considered before applying the default deny.

```
ufw allow git

ufw allow in http

ufw allow out http <- required for apt to connect to repository

ufw allow in https

ufw allow out https

ufw allow out 53

ufw logging on
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.2 Configure nftables

If Uncomplicated Firewall (UFW) or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables. The biggest change with the successor nftables is its simplicity. With iptables, we have to configure every single rule and use the syntax which can be compared with normal commands. With nftables, the simpler syntax, much like BPF (Berkely Packet Filter) means shorter lines and less repetition. Support for nftables should also be compiled into the kernel, together with the related nftables modules. Please ensure that your kernel supports nf_tables before choosing this option.

Note:

- This section broadly assumes starting with an empty nftables firewall ruleset (established by flushing the rules with nft flush ruleset).
- Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot.
- Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

The following will implement the firewall rules of this section and open ICMP, IGMP, and port 22(ssh) from anywhere. Opening the ports for ICMP, IGMP, and port 22(ssh) needs to be updated in accordance with local site policy. **Allow port 22(ssh) needs to be updated to only allow systems requiring ssh connectivity to connect, as per site policy** .

Save the script bellow as `/etc/nftables.rules`

```
#!/sbin/nft -f
```

```
# This nftables.rules config should be saved as /etc/nftables.rules

# flush nftables 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


# 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.rules
```

All changes in the nftables subsections are temporary.

To make these changes permanent:

Run the following command to create the nftables.rules file

```
nft list ruleset > /etc/nftables.rules
```

Add the following line to `/etc/nftables.conf`

```
include "/etc/nftables.rules"
```

3.4.2.1 Ensure nftables is installed

Fail

Description:

nftables provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM) and a new nft userspace command line tool. nftables reuses the existing Netfilter subsystems such as the existing hook infrastructure, the connection tracking system, NAT, userspace queuing and logging subsystem.

Notes:

- *nftables is available in Linux kernel 3.13 and newer*
- *Only one firewall utility should be installed and configured*
- *Changing firewall settings while connected over the network can result in being locked out of the system*

Rationale:

nftables is a subsystem of the Linux kernel that can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

Remediation:

Run the following command to install `nftables` :

```
# apt install nftables
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.2.2 Ensure ufw is uninstalled or disabled with nftables

Pass

Description:

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

Rationale:

Running both the `nftables` service and `ufw` may lead to conflict and unexpected results.

Remediation:

Run **one** of the following to either remove `ufw` **or** disable `ufw` and mask `ufw.service` :

Run the following command to remove `ufw` :

```
# apt purge ufw
```

-OR-

Run the following commands to disable `ufw` and mask `ufw.service` :

```
# ufw disable

# systemctl stop ufw.service

# systemctl mask ufw.service
```

Note: `ufw disable` needs to be run before `systemctl mask ufw.service` in order to correctly disable `UFW`

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.2.3 Ensure iptables are flushed with nftables

Manual

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

Remediation:

Run the following commands to flush iptables:

For iptables:

```
# iptables -F
```

For ip6tables:

```
# ip6tables -F
```

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

3.4.2.4 Ensure a nftables table exists

Fail

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.

Remediation:

Run the following command to create a table in nftables

```
# nft create table inet <table name>
```

Example:

```
# nft create table inet filter
```

Impact:

Adding rules to a running nftables can cause loss of connectivity to the system

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

3.4.2.5 Ensure nftables base chains exist

Fail

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.

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 \; }
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.2.6 Ensure nftables loopback traffic is configured

Fail

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.

Remediation:

Run the following commands to implement the loopback rules:

```
# nft add rule inet filter input iif lo accept
# nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop
```

-IF- IPv6 is enabled on the system:

Run the following command to implement the IPv6 loopback rule:

```
# nft add rule inet filter input ip6 saddr ::1 counter drop
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.2.7 Ensure nftables outbound and established connections are configured

Manual

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.

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
```

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.2.8 Ensure nftables default deny firewall policy

Fail

Description:

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

Rationale:

There are two policies: accept (Default) and drop. If the policy is set to `accept` , the firewall will accept any packet that is not configured to be denied and the packet will continue transversing the network stack.

It is easier to white list acceptable usage than to black list unacceptable usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

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 \; }
```

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** Manual Page nft
- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.2.9 Ensure nftables service is enabled

Fail

Description:

The nftables service allows for the loading of nftables rulesets during boot, or starting on the nftables service

Rationale:

The nftables service restores the nftables rules from the rules files referenced in the `/etc/nftables.conf` file during boot or the starting of the nftables service

Remediation:

Run the following command to enable the nftables service:

```
# systemctl enable nftables
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.2.10 Ensure nftables rules are permanent

Fail

Description:

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames.

The nftables service reads the `/etc/nftables.conf` file for a nftables file or files to include in the nftables ruleset.

A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.

Rationale:

Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot

Remediation:

Edit the `/etc/nftables.conf` file and un-comment or add a line with `include <Absolute path to nftables rules file>` for each nftables file you want included in the nftables ruleset on boot

Example:

```
# vi /etc/nftables.conf
```

Add the line:

```
include "/etc/nftables.rules"
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.3 Configure iptables

If Uncomplicated Firewall (UFW) or nftables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

IPtables is an application that allows a system administrator to configure the IPv4 and IPv6 tables, chains and rules provided by the Linux kernel firewall. While several methods of configuration exist this section is intended only to ensure the resulting IPtables rules are in place, not how they are configured. If IPv6 is in use in your environment, similar settings should be applied to the IP6tables as well.

Note: Configuration of a live system's firewall directly over a remote connection will often result in being locked out

3.4.3.1 Configure iptables software

This section provides guidance for installing, enabling, removing, and disabling software packages necessary for using IPTables as the method for configuring and maintaining a Host Based Firewall on the system.

Note: Using more than one method to configure and maintain a Host Based Firewall can cause unexpected results. If FirewallD or NFTables are being used for configuration and maintenance, this section should be skipped and the guidance in their respective section followed.

3.4.3.1.1 Ensure iptables packages are installed

Fail

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.

Remediation:

Run the following command to install `iptables` and `iptables-persistent`

```
# apt install iptables iptables-persistent
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.3.1.2 Ensure nftables is not installed with iptables

Pass

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.

Remediation:

Run the following command to remove `nftables` :

```
# apt purge nftables
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, CM-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.3.1.3 Ensure ufw is uninstalled or disabled with iptables

Pass

Description:

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

- Uses a command-line interface consisting of a small number of simple commands
- Uses iptables for configuration

Rationale:

Running `iptables.persistent` with ufw enabled may lead to conflict and unexpected results.

Remediation:

Run *one* of the following commands to either remove `ufw` or stop and mask `ufw`

Run the following command to remove `ufw` :

```
# apt purge ufw
```

-OR-

Run the following commands to disable `ufw` :

```
# ufw disable

# systemctl stop ufw

# systemctl mask ufw
```

Note:`ufw disable` needs to be run before `systemctl mask ufw` in order to correctly disable `UFW`

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.3.2 Configure IPv4 iptables

Iptables is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

Note: This section broadly assumes starting with an empty IPtables firewall ruleset (established by flushing the rules with iptables -F). Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot. Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot. The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere:

```
#!/bin/bash


# Flush IPtables rules

iptables -F


# Ensure default deny firewall policy

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP


# Ensure loopback traffic is configured

iptables -A INPUT -i lo -j ACCEPT

iptables -A OUTPUT -o lo -j ACCEPT

iptables -A INPUT -s 127.0.0.0/8 -j DROP


# Ensure outbound and established connections are configured

iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT

iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT

iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT


# Open inbound ssh(tcp port 22) connections

iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

3.4.3.2.1 Ensure iptables default deny firewall policy

Fail

Description:

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Notes:

- *Changing firewall settings while connected over network can result in being locked out of the system*
- *Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well*

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Remediation:

Run the following commands to implement a default DROP policy:

```
# iptables -P INPUT DROP

# iptables -P OUTPUT DROP

# iptables -P FORWARD DROP
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.3.2.2 Ensure iptables loopback traffic is configured

Fail

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).

Notes:

- *Changing firewall settings while connected over network can result in being locked out of the system*
- *Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well*

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

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
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.3.2.3 Ensure iptables outbound and established connections are configured

Manual

Description:

Configure the firewall rules for new outbound, and established connections.

Notes:

- *Changing firewall settings while connected over network can result in being locked out of the system*
- *Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well*

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

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
```

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.3.2.4 Ensure iptables firewall rules exist for all open ports

Fail

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Note:

- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well
- The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

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
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.3.3 Configure IPv6 ip6tables

Ip6tables is used to set up, maintain, and inspect the tables of IPv6 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a `target', which may be a jump to a user-defined chain in the same table.

If IPv6 in enabled on the system, the ip6tables should be configured.

Note: This section broadly assumes starting with an empty ip6tables firewall ruleset (established by flushing the rules with ip6tables -F). Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot. Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere:

```
#!/bin/bash


# Flush ip6tables rules

ip6tables -F


# Ensure default deny firewall policy

ip6tables -P INPUT DROP

ip6tables -P OUTPUT DROP

ip6tables -P FORWARD DROP


# Ensure loopback traffic is configured

ip6tables -A INPUT -i lo -j ACCEPT

ip6tables -A OUTPUT -o lo -j ACCEPT

ip6tables -A INPUT -s ::1 -j DROP


# Ensure outbound and established connections are configured

ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT

ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
ip6tables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT

ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT

ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT

ip6tables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT


# Open inbound ssh(tcp port 22) connections

ip6tables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

3.4.3.3.1 Ensure ip6tables default deny firewall policy

Fail

Description:

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Note:

- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Remediation:

IF IPv6 is enabled on your system:

Run the following commands to implement a default DROP policy:

```
# ip6tables -P INPUT DROP

# ip6tables -P OUTPUT DROP

# ip6tables -P FORWARD DROP
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.3.3.2 Ensure ip6tables loopback traffic is configured

Pass

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1).

Note:

- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

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
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.3.3.3 Ensure ip6tables outbound and established connections are configured

Manual

Description:

Configure the firewall rules for new outbound, and established IPv6 connections.

Note:

- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

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
```

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

3.4.3.3.4 Ensure ip6tables firewall rules exist for all open ports

Fail

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Note:

- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well
- The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

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
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CA-9, SC-7

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

4 Access, Authentication and Authorization

4.1 Configure time-based job schedulers

`cron` is a time-based job scheduler used to schedule jobs, commands or shell scripts, to run periodically at fixed times, dates, or intervals.

`at` provides the ability to execute a command or shell script at a specified date and hour, or after a given interval of time.

Notes:

- *Other methods exist for scheduling jobs, such as* `systemd timers` *. If another method is used, it should be secured in accordance with local site policy*
- `systemd timers` *are systemd unit files whose name ends in* `.timer` *that control* `.service` *files or events*

- *Timers can be used as an alternative to* `cron` *and* `at`
- *Timers have built-in support for calendar time events, monotonic time events, and can be run asynchronously*

- *If* `cron` *and* `at` *are not installed, this section can be skipped*

4.1.1 Ensure cron daemon is enabled and active

Pass

Description:

The `cron` daemon is used to execute batch jobs on the system.

Note: Other methods, such as `systemd timers` , exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and `cron` is used to execute them.

Remediation:

Run the following command to enable and start `cron` :

```
# systemctl unmask cron

# systemctl --now enable cron
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Back to Summary

4.1.2 Ensure permissions on /etc/crontab are configured

Pass

Description:

The `/etc/crontab` file is used by `cron` to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file.

Note: Other methods, such as `systemd timers` , exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Remediation:

Run the following commands to set ownership and permissions on `/etc/crontab` :

```
# chown root:root /etc/crontab

# chmod og-rwx /etc/crontab
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
>

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
>

Back to Summary

4.1.3 Ensure permissions on /etc/cron.hourly are configured

Fail

Description:

This directory contains system `cron` jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Note: Other methods, such as `systemd timers` , exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

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/
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
>

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
>

Back to Summary

4.1.4 Ensure permissions on /etc/cron.daily are configured

Fail

Description:

The `/etc/cron.daily` directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Note: Other methods, such as `systemd timers` , exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.daily` directory:

```
# chown root:root /etc/cron.daily/

# chmod og-rwx /etc/cron.daily/
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
  >

Back to Summary

4.1.5 Ensure permissions on /etc/cron.weekly are configured

Fail

Description:

The `/etc/cron.weekly` directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Note: Other methods, such as `systemd timers` , exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.weekly` directory:

```
# chown root:root /etc/cron.weekly/

# chmod og-rwx /etc/cron.weekly/
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
  >

Back to Summary

4.1.6 Ensure permissions on /etc/cron.monthly are configured

Fail

Description:

The `/etc/cron.monthly` directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Note: Other methods, such as `systemd timers` , exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.monthly` directory:

```
# chown root:root /etc/cron.monthly/

# chmod og-rwx /etc/cron.monthly/
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
>

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
>

Back to Summary

4.1.7 Ensure permissions on /etc/cron.d are configured

Fail

Description:

The `/etc/cron.d` directory contains system `cron` jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from `/etc/crontab` , but require more granular control as to when they run. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Note: Other methods, such as `systemd timers` , exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.d` directory:

```
# chown root:root /etc/cron.d/

# chmod og-rwx /etc/cron.d/
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

4.1.8 Ensure cron is restricted to authorized users

Fail

Description:

Configure `/etc/cron.allow` to allow specific users to use this service. If `/etc/cron.allow` does not exist, then `/etc/cron.deny` is checked. Any user not specifically defined in this file is allowed to use cron. By removing the file, only users in `/etc/cron.allow` are allowed to use cron.

Note:

- Other methods, such as `systemd timers` , exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy
- 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.

Remediation:

Run the following script to:

- Remove `/etc/cron.deny` if it exists
- Create `/etc/cron.allow` if it doesn't exist
- Change ownership of `/etc/cron.allow` to the `root` user
- Change group ownership of `/etc/cron.allow` to the group `crontab`

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



{

if dpkg-query -W cron > /dev/null 2>&1; then

l_file="/etc/cron.allow"

l_mask='0137'

l_maxperm="$( printf '%o' $(( 0777 & ~$l_mask)) )"

if [ -e /etc/cron.deny ]; then

echo -e " - Removing \"/etc/cron.deny\""

rm -f /etc/cron.deny

fi

if [ ! -e /etc/cron.allow ]; then

echo -e " - creating \"$l_file\""

touch "$l_file"
```

```
fi
while read l_mode l_fown l_fgroup; do
if [ $(( $l_mode & $l_mask )) -gt 0 ]; then
echo -e " - Removing excessive permissions from \"$l_file\""
chmod u-x,g-wx,o-rwx "$l_file"
fi
if [ "$l_fown" != "root" ]; then
echo -e " - Changing owner on \"$l_file\" from: \"$l_fown\" to: \"root\""
chown root "$l_file"
fi
if [ "$l_fgroup" != "crontab" ]; then
echo -e " - Changing group owner on \"$l_file\" from: \"$l_fgroup\" to: \"crontab\""
chgrp crontab "$l_file"
fi
done < <(stat -Lc '%#a %U %G' "$l_file")
else
echo -e "- cron is not installed on the system, no remediation required\n"
fi
}
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

4.1.9 Ensure at is restricted to authorized users

Pass

Description:

Configure `/etc/at.allow` to allow specific users to use this service. If `/etc/at.allow` does not exist, then `/etc/at.deny` is checked. Any user not specifically defined in this file is allowed to use `at` . By removing the file, only users in `/etc/at.allow` are allowed to use `at` .

Note: Other methods, such as `systemd timers` , exist for scheduling jobs. If another method is used, `at` should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

On many systems, only the system administrator is authorized to schedule `at` jobs. Using the `at.allow` file to control who can run `at` jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Remediation:

Run the following script to:

- Remove `/etc/at.deny` if it exists
- Create `/etc/at.allow` if it doesn't exist
- Change ownership of `/etc/at.allow` to the `root` user
- Change group ownership of `/etc/at.allow` to the group `root`

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


{
if dpkg-query -W at > /dev/null 2>&1; then
l_file="/etc/at.allow"
l_mask='0137'
l_maxperm="$( printf '%o' $(( 0777 & ~$l_mask)) )"
if [ -e /etc/at.deny ]; then
echo -e " - Removing \"/etc/at.deny\""
rm -f /etc/at.deny
fi
if [ ! -e /etc/at.allow ]; then
echo -e " - creating \"$l_file\""
touch "$l_file"
fi
while read l_mode l_fown l_fgroup; do
if [ $(( $l_mode & $l_mask )) -gt 0 ]; then
echo -e " - Removing excessive permissions from \"$l_file\""
chmod u-x,g-wx,o-rwx "$l_file"
fi
if [ "$l_fown" != "root" ]; then
echo -e " - Changing owner on \"$l_file\" from: \"$l_fown\" to: \"root\""
chown root "$l_file"
fi
if [ "$l_fgroup" != "root" ]; then
echo -e " - Changing group owner on \"$l_file\" from: \"$l_fgroup\" to: \"root\""
chgrp root "$l_file"
fi
done < <(stat -Lc '%#a %U %G' "$l_file")
else
echo -e "- cron is not installed on the system, no remediation required\n"
fi
}
```

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
>

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
>

Back to Summary

4.2 Configure SSH Server

SSH is a secure, encrypted replacement for common login services such as `telnet`, `ftp`, `rlogin`, `rsh`, and `rcp`. It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

Note:

- The recommendations in this section only apply if the SSH daemon is installed on the system, if remote access is **not** required the SSH daemon can be removed and this section skipped.
- The following openSSH daemon configuration options, `Include` and `Match`, may cause the audits in this section's recommendations to report incorrectly. It is recommended that these options only be used if they're needed and fully understood. If these options are configured in accordance with local site policy, they should be accounted for when following the recommendations in this section.
- The default `Include` location is the `/etc/ssh/sshd_config.d` directory. This default has been accounted for in this section. If a file has an additional `Include` that isn't this default location, the files should be reviewed to verify that the recommended setting is not being over-ridden.
- The audits of the running configuration in this section are run in the context of the root user, the local host name, and the local host's IP address. If a `Match` block exists that matches one of these criteria, the output of the audit will be from the match block. The respective matched criteria should be replaced with a non-matching substitution.
- Once all configuration changes have been made to `/etc/ssh/sshd_config` or any included configuration files, the `sshd` configuration must be reloaded
- `Include:`
  - Include the specified configuration file(s).
  - Multiple pathnames may be specified and each pathname may contain glob(7) wildcards.
  - Files without absolute paths are assumed to be in /etc/ssh.
  - An Include directive may appear inside a Match block to perform conditional inclusion.
- `Match:`
  - Introduces a conditional block.
  - If all of the criteria on the Match line are satisfied, the keywords on the following lines override those set in the global section of the config file, until either another Match line or the end of the file.
  - If a keyword appears in multiple Match blocks that are satisfied, only the first instance of the keyword is applied.
  - The arguments to Match are one or more criteria-pattern pairs or the single token All which matches all criteria. The available criteria are User, Group, Host, LocalAddress, LocalPort, RDomain, and Address (with RDomain representing the rdomain(4) on which the connection was received).
  - The match patterns may consist of single entries or comma-separated lists and may use the wildcard and negation operators described in the PATTERNS section of ssh_config(5).
  - The patterns in an Address criteria may additionally contain addresses to match in CIDR address/masklen format, such as 192.0.2.0/24 or 2001:db8::/32. Note that the mask length provided must be consistent with the address - it is an error to specify a mask length that is too long for the address or one with bits set in this host portion of the address. For example, 192.0.2.0/33 and 192.0.2.0/8, respectively.
  - Only a subset of keywords may be used on the lines following a Match keyword.
  - Available keywords are: `AcceptEnv`, `AllowAgentForwarding`, `AllowGroups`, `AllowStreamLocalForwarding`, `AllowTcpForwarding`, `AllowUsers`, `AuthenticationMethods`, `AuthorizedKeysCommand`, `AuthorizedKeysCommandUser`, `AuthorizedKeysFile`, `AuthorizedPrincipalsCommand`, `AuthorizedPrincipalsCommandUser`, `AuthorizedPrincipalsFile`, `Banner`, `ChrootDirectory`, `ClientAliveCountMax`, `ClientAliveInterval`, `DenyGroups`, `DenyUsers`, `ForceCommand`, `GatewayPorts`, `GSSAPIAuthentication`, `HostbasedAcceptedKeyTypes`, `HostbasedAuthentication`, `HostbasedUsesNameFromPacketOnly`, `Include`, `IPQoS`, `KbdInteractiveAuthentication`, `KerberosAuthentication`, `LogLevel`, `MaxAuthTries`, `MaxSessions`, `PasswordAuthentication`, `PermitEmptyPasswords`, `PermitListen`, `PermitOpen`, `PermitRootLogin`, `PermitTTY`, `PermitTunnel`, `PermitUserRC`, `PubkeyAcceptedKeyTypes`, `PubkeyAuthentication`, `RekeyLimit`, `RevokedKeys`, `RDomain`, `SetEnv`, `StreamLocalBindMask`, `StreamLocalBindUnlink`, `TrustedUserCAKeys`, `X11DisplayOffset`, `X11Forwarding` and `X11UseLocalhost`.

Command to re-load the SSH daemon configuration:

```
# systemctl reload sshd
```

Command to remove the SSH daemon:

```
# apt purge openssh-server
```

4.2.1 Ensure permissions on /etc/ssh/sshd_config are configured

Fail

Description:

The file `/etc/ssh/sshd_config` , and files ending in `.conf` in the `/etc/ssh/sshd_config.d` directory, contain configuration specifications for `sshd` .

Rationale:

configuration specifications for `sshd` need to be protected from unauthorized changes by non-privileged users.

Remediation:

Run the following script to set ownership and permissions on `/etc/ssh/sshd_config` and files ending in `.conf` in the `/etc/ssh/sshd_config.d` directory:

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



{

chmod u-x,og-rwx /etc/ssh/sshd_config

chown root:root /etc/ssh/sshd_config

while IFS= read -r -d $'\0' l_file; do

if [ -e "$l_file" ]; then

chmod u-x,og-rwx "$l_file"

chown root:root "$l_file"

fi

done < <(find /etc/ssh/sshd_config.d -type f -print0)

}
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

4.2.2 Ensure permissions on SSH private host key files are configured

Pass

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

Remediation:

Run the following script to set mode, ownership, and group on the private SSH host key files:

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

```
{

l_output="" l_output2=""

l_skgn="ssh_keys" # Group designated to own openSSH keys

l_skgid="$(awk -F: '($1 == "'"$l_skgn"'"){print $3}' /etc/group)" # Get gid of group

if [ -n "$l_skgid" ]; then

l_agroup="(root|$l_skgn)" && l_sgroup="$l_skgn" && l_mfix="u-x,g-wx,o-rwx"

else

l_agroup="root" && l_sgroup="root" && l_mfix="u-x,go-rwx"

fi

unset a_skarr && a_skarr=() # Clear and initialize array

while IFS= read -r -d $'\0' l_file; do # Loop to populate array

if grep -Pq ':\h+OpenSSH\h+private\h+key\b' <<< "$(file "$l_file")"; then

a_skarr+=("$(stat -Lc '%n^%#a^%U^%G^%g' "$l_file")")

fi

done < <(find -L /etc/ssh -xdev -type f -print0)

while IFS="^" read -r l_file l_mode l_owner l_group l_gid; do

l_out2=""

[ "$l_gid" = "$l_skgid" ] && l_pmask="0137" || l_pmask="0177"

l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"

if [ $(( $l_mode & $l_pmask )) -gt 0 ]; then

l_out2="$l_out2\n - Mode: \"$l_mode\" should be mode: \"$l_maxperm\" or more restrictive\n - Revoking
excess permissions"

chmod "$l_mfix" "$l_file"

fi

if [ "$l_owner" != "root" ]; then

l_out2="$l_out2\n - Owned by: \"$l_owner\" should be owned by \"root\"\n - Changing ownership to
\"root\""

chown root "$l_file"

fi

if [[ ! "$l_group" =~ $l_agroup ]]; then

l_out2="$l_out2\n - Owned by group \"$l_group\" should be group owned by: \"${l_agroup//|/ or }\"\n -
Changing group ownership to \"$l_sgroup\""

chgrp "$l_sgroup" "$l_file"

fi

[ -n "$l_out2" ] && l_output2="$l_output2\n - File: \"$l_file\"$l_out2"

done <<< "$(printf '%s\n' "${a_skarr[@]}")"

unset a_skarr

if [ -z "$l_output2" ]; then

echo -e "\n- No access changes required\n"

else

echo -e "\n- Remediation results:\n$l_output2\n"

fi

}
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

4.2.3 Ensure permissions on SSH public host key files are configured

Pass

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.

Remediation:

Run the following script to set mode, ownership, and group on the public SSH host key files:

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


{

l_pmask="0133"

l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"

awk '{print}' <<< "$(find -L /etc/ssh -xdev -type f -exec stat -Lc "%n %#a %U %G" {} +)" | (while read -
r l_file l_mode l_owner l_group; do

if file "$l_file" | grep -Pq ':\h+OpenSSH\h+(\H+\h+)?public\h+key\b'; then

echo -e " - Checking private key file: \"$l_file\""

if [ $(( $l_mode & $l_pmask )) -gt 0 ]; then

echo -e " - File: \"$l_file\" is mode \"$l_mode\" changing to mode: \"$l_maxperm\""

chmod u-x,go-wx "$l_file"

fi

if [ "$l_owner" != "root" ]; then

echo -e " - File: \"$l_file\" is owned by: \"$l_owner\" changing owner to \"root\""

chown root "$l_file"

fi

if [ "$l_group" != "root" ]; then

echo -e " - File: \"$l_file\" is owned by group \"$l_group\" changing to group \"root\""

chgrp "root" "$l_file"

fi

fi

done

)
```

```
}
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

4.2.4 Ensure SSH access is limited

Fail

Description:

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

- `AllowUsers`:
  - The `AllowUsers` variable gives the system administrator the option of allowing specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.
- `AllowGroups`:
  - The `AllowGroups` variable gives the system administrator the option of allowing specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.
- `DenyUsers`:
  - The `DenyUsers` variable gives the system administrator the option of denying specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.
- `DenyGroups`:
  - The `DenyGroups` variable gives the system administrator the option of denying specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

Rationale:

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set one or more of the parameter above any `Include` entries as follows:

```
AllowUsers <userlist>
```

OR

```
AllowGroups <grouplist>
```

OR

```
DenyUsers <userlist>
```

OR

```
DenyGroups <grouplist>
```

Note: First occurrence of a option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location. If the `Include` location is not the default, `/etc/ssh/sshd_config.d/*.conf` , the audit will need to be modified to account for the `Include` location used.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SSHD_CONFIG(5)
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

4.2.5 Ensure SSH LogLevel is appropriate

Pass

Description:

`INFO` level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

`VERBOSE` level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments.

Rationale:

SSH provides several logging levels with varying amounts of verbosity. `DEBUG` is specifically **not** recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
LogLevel VERBOSE
```

OR

```
LogLevel INFO
```

Note: First occurrence of a option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://www.ssh.com/ssh/sshd_config/
- **URL:** NIST SP 800-53 Rev. 5: AU-3, AU-12, SI-5

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

4.2.6 Ensure SSH PAM is enabled

Pass

Description:

The `UsePAM` directive enables the Pluggable Authentication Module (PAM) interface. If set to `yes` this will enable PAM authentication using `ChallengeResponseAuthentication` and `PasswordAuthentication` directives in addition to PAM account and session module processing for all authentication types.

Rationale:

When `usePAM` is set to `yes` , PAM runs through account and session types properly. This is important if you want to restrict access to services based off of IP, time or other factors of the account. Additionally, you can make sure users inherit certain environment variables on login or disallow access to the server

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
UsePAM yes
```

Note: First occurrence of a option takes precedence. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SSHD_CONFIG(5)
- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.2.7 Ensure SSH root login is disabled

Fail

Description:

The `PermitRootLogin` parameter specifies if the root user can log in using SSH. The default is `prohibit-password` .

Rationale:

Disallowing `root` logins over SSH requires system admins to authenticate using their own individual account, then escalating to `root` . This limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
PermitRootLogin no
```

Note: First occurrence of a option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SSHD_CONFIG(5)

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.2.8 Ensure SSH HostbasedAuthentication is disabled

Pass

Description:

The `HostbasedAuthentication` parameter specifies if authentication is allowed through trusted hosts via the user of `.rhosts` , or `/etc/hosts.equiv` , along with successful public key client host authentication.

Rationale:

Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf` , disabling the ability to use `.rhosts` files in SSH provides an additional layer of protection.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
HostbasedAuthentication no
```

Note: First occurrence of a option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SSHD_CONFIG(5)

Back to Summary

4.2.9 Ensure SSH PermitEmptyPasswords is disabled

Pass

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.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
PermitEmptyPasswords no
```

Note: First occurrence of a option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SSHD_CONFIG(5)

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.2.10 Ensure SSH PermitUserEnvironment is disabled

Pass

Description:

The `PermitUserEnvironment` option allows users to present environment options to the SSH daemon.

Rationale:

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has SSH executing trojan'd programs)

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any Include entries as follows:

```
PermitUserEnvironment no
```

Note: First occurrence of a option takes precedence. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SSHD_CONFIG(5)

Back to Summary

4.2.11 Ensure SSH IgnoreRhosts is enabled

Pass

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.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any Include entries as follows:

```
IgnoreRhosts yes
```

Note: First occurrence of a option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SSHD_CONFIG(5)

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.2.13 Ensure only strong Ciphers are used

Pass

Description:

This variable limits the ciphers that SSH can use during communication.

Note:

- Some organizations may have stricter requirements for approved ciphers.
- Ensure that ciphers used are in compliance with site policy.
- The only "strong" ciphers currently FIPS 140-2 compliant are:
  - aes256-ctr
  - aes192-ctr
  - aes128-ctr

Rationale:

Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised.

- The Triple DES ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain clear text data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack.
- Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plain text data from an arbitrary block of cipher text in an SSH session via unknown vectors.

Remediation:

Edit the `/etc/ssh/sshd_config` file add/modify the `Ciphers` line to contain a comma separated list of the site approved ciphers above any `Include` entries:

Example:

```
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
```

Note: First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://nvd.nist.gov/vuln/detail/CVE-2016-2183
- **URL:** https://www.openssh.com/txt/cbc.adv
- **URL:** https://nvd.nist.gov/vuln/detail/CVE-2008-5161
- **URL:** https://www.openssh.com/txt/cbc.adv
- **URL:** SSHD_CONFIG(5)

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
  >

Back to Summary

4.2.14 Ensure only strong MAC algorithms are used

Pass

Description:

This variable limits the types of MAC algorithms that SSH can use during communication.

Notes:

- Some organizations may have stricter requirements for approved MACs.
- Ensure that MACs used are in compliance with site policy.
- The only "strong" MACs currently FIPS 140-2 approved are:
  - hmac-sha2-256
  - hmac-sha2-512

Rationale:

MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information.

Remediation:

Edit the `/etc/ssh/sshd_config` file and add/modify the MACs line to contain a comma separated list of the site approved MACs above any `Include` entries:

Example:

```
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128-etm@openssh.com,umac-128@openssh.com
```

Note: First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** More information on SSH downgrade attacks can be found here: http://www.mitls.org/pages/attacks/SLOTH
- **URL:** SSHD_CONFIG(5)
- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
- **Control 16: Account Monitoring and Control:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
  >

Back to Summary

4.2.15 Ensure only strong Key Exchange algorithms are used

Pass

Description:

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received

Notes:

- Kex algorithms have a higher preference the earlier they appear in the list
- Some organizations may have stricter requirements for approved Key exchange algorithms
- Ensure that Key exchange algorithms used are in compliance with site policy

- The only Key Exchange Algorithms currently FIPS 140-2 approved are:
  - ecdh-sha2-nistp256
  - ecdh-sha2-nistp384
  - ecdh-sha2-nistp521
  - diffie-hellman-group-exchange-sha256
  - diffie-hellman-group16-sha512
  - diffie-hellman-group18-sha512
  - diffie-hellman-group14-sha256

Rationale:

Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

Remediation:

Edit the /etc/ssh/sshd_config file add/modify the KexAlgorithms line to contain a comma separated list of the site approved key exchange algorithms above any `Include` entries:

Example:

```
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
```

Note: First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: SC-8

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

4.2.17 Ensure SSH warning banner is configured

Pass

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.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
Banner /etc/issue.net
```

Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Back to Summary

4.2.18 Ensure SSH MaxAuthTries is set to 4 or less

Fail

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.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
MaxAuthTries 4
```

Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SSHD_CONFIG(5)
- **URL:** NIST SP 800-53 Rev. 5: AU-3

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

4.2.19 Ensure SSH MaxStartups is configured

Fail

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.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
MaxStartups 10:30:60
```

Note: First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SSHD_CONFIG(5)
- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

4.2.20 Ensure SSH LoginGraceTime is set to one minute or less

Fail

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.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
LoginGraceTime 60
```

Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SSHD_CONFIG(5)
- **URL:** NIST SP 800-53 Rev. 5: CM-6

Back to Summary

4.2.21 Ensure SSH MaxSessions is set to 10 or less

Pass

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.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
MaxSessions 10
```

Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SSHD_CONFIG(5)
- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Back to Summary

4.2.22 Ensure SSH Idle Timeout Interval is configured

Pass

Description:

Note: To clarify, the two settings described below are only meant for idle connections from a protocol perspective and are not meant to check if the user is active or not. An idle user does not mean an idle connection. SSH does not and never had, intentionally, the capability to drop idle users. In SSH versions before `8.2p1` there was a bug that caused these values to behave in such a manner that they were abused to disconnect idle users. This bug has been resolved in `8.2p1` and thus it can no longer be abused disconnect idle users.

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of SSH sessions. Taken directly from `man 5 sshd_config`:

- `ClientAliveInterval` Sets a timeout interval in seconds after which if no data has been received from the client, sshd(8) will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client.
- `ClientAliveCountMax` Sets the number of client alive messages which may be sent without sshd(8) receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. It is important to note that the use of client alive messages is very different from TCPKeepAlive. The client alive messages are sent through the encrypted channel and therefore will not be spoofable. The TCP keepalive option en-abled by TCPKeepAlive is spoofable. The client alive mechanism is valuable when the client or server depend on knowing when a connection has become unresponsive. The default value is 3. If ClientAliveInterval is set to 15, and ClientAliveCountMax is left at the default, unresponsive SSH clients will be disconnected after approximately 45 seconds. Setting a zero ClientAliveCountMax disables connection termination.

Rationale:

In order to prevent resource exhaustion, appropriate values should be set for both `ClientAliveInterval` and `ClientAliveCountMax`. Specifically, looking at the source code, `ClientAliveCountMax` must be greater than zero in order to utilize the ability of SSH to drop idle connections. If connections are allowed to stay open indefinately, this can potentially be used as a DDOS attack or simple resource exhaustion could occur over unreliable networks.

The example set here is a 45 second timeout. Consult your site policy for network timeouts and apply as appropriate.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameters above any `Include` entries according to site policy.

Example:

```
ClientAliveInterval 15

ClientAliveCountMax 3
```

Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://man.openbsd.org/sshd_config
- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Back to Summary

4.3 Configure privilege escalation

There are various tools which allows a permitted user to execute a command as the superuser or another user, as specified by the security policy.

sudo

sudo documentation

The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

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

pkexec

pkexec documentation

`pkexec` allows an authorized user to execute *PROGRAM* as another user. If *username* is not specified, then the program will be executed as the administrative super user, `root` .

4.3.1 Ensure sudo is installed

Pass

Description:

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

Rationale:

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

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

Remediation:

First determine is LDAP functionality is required. If so, then install `sudo-ldap` , else install `sudo` .

Example:

```
# apt install sudo
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SUDO(8)
- **URL:** NIST SP 800-53 Rev. 5: AC-2, AC-6

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More
  >

Back to Summary

4.3.2 Ensure sudo commands use pty

Fail

Description:

`sudo` can be configured to run only from a pseudo terminal (`pseudo-pty`).

Rationale:

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

Remediation:

Edit the file `/etc/sudoers` with `visudo` or a file in `/etc/sudoers.d/` with `visudo -f <PATH TO FILE>` and add the following line:

```
Defaults use_pty
```

Note:

- sudo will read each file in `/etc/sudoers.d` , skipping file names that end in `~` or contain a `.` character to avoid causing problems with package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, `/etc/sudoers.d/01_first` will be parsed before `/etc/sudoers.d/10_second`.
- Be aware that because the sorting is lexical, not numeric, `/etc/sudoers.d/1_whoops` would be loaded after `/etc/sudoers.d/10_second`.
- Using a consistent number of leading zeroes in the file names can be used to avoid such problems.

Impact:

WARNING: Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SUDO(8)
- **URL:** VISUDO(8)
- **URL:** sudoers(5)

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More
  >

Back to Summary

4.3.3 Ensure sudo log file exists

Fail

Description:

sudo can use a custom log file

Rationale:

A sudo log file simplifies auditing of sudo commands

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo` or `visudo -f <PATH TO FILE>` and add the following line:

Example:

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

Note:

- sudo will read each file in `/etc/sudoers.d`, skipping file names that end in `~` or contain a `.` character to avoid causing problems with package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, `/etc/sudoers.d/01_first` will be parsed before `/etc/sudoers.d/10_second`.
- Be aware that because the sorting is lexical, not numeric, `/etc/sudoers.d/1_whoops` would be loaded after `/etc/sudoers.d/10_second`.
- Using a consistent number of leading zeroes in the file names can be used to avoid such problems.

Impact:

WARNING: Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** SUDO(8)
- **URL:** VISUDO(8)
- **URL:** sudoers(5)

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

4.3.5 Ensure re-authentication for privilege escalation is not disabled globally

Pass

Description:

The operating system must be configured so that users must re-authenticate for privilege escalation.

Rationale:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Remediation:

Configure the operating system to require users to reauthenticate for privilege escalation.

Based on the outcome of the audit procedure, use `visudo -f <PATH TO FILE>` to edit the relevant sudoers file.

Remove any occurrences of `!authenticate` tags in the file(s).

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AC-6

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.3.6 Ensure sudo authentication timeout is configured correctly

Pass

Description:

`sudo` caches used credentials for a default of 15 minutes. This is for ease of use when there are multiple administrative tasks to perform. The timeout can be modified to suit local security policies.

This default is distribution specific. See audit section for further information.

Rationale:

Setting a timeout value reduces the window of opportunity for unauthorized privileged access to another user.

Remediation:

If the currently configured timeout is larger than 15 minutes, edit the file listed in the audit section with `visudo -f <PATH TO FILE>` and modify the entry `timestamp_timeout=` to 15 minutes or less as per your site policy. The value is in minutes. This particular entry may appear on it's own, or on the same line as `env_reset` . See the following two examples:

```
Defaults env_reset, timestamp_timeout=15
```

```
Defaults timestamp_timeout=15

Defaults env_reset
```

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://www.sudo.ws/man/1.9.0/sudoers.man.html
- **URL:** NIST SP 800-53 Rev. 5: AC-6

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.3.7 Ensure access to the su command is restricted

Fail

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.

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
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

4.4 Configure PAM

PAM (Pluggable Authentication Modules) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the `/etc/pam.d` directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

Note: The usage of `pam-auth-update` :

- As of this writing, the management of PAM via `pam-auth-update` does not offer all the required functionality implemented by the benchmark. As such, the usage of `pam-auth-update` is not recommended at present.

4.4.1 Ensure password creation requirements are configured

Fail

Description:

The `pam_pwquality.so` module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.

The following options are set in the `/etc/security/pwquality.conf` file:

- Password Length:
  - `minlen = 14` - password must be 14 characters or more
- Password complexity:
  - `minclass = 4` - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

    OR

  - `dcredit = -1` - provide at least one digit
  - `ucredit = -1` - provide at least one uppercase character
  - `ocredit = -1` - provide at least one special character
  - `lcredit = -1` - provide at least one lowercase character

Rationale:

Strong passwords protect systems from being hacked through brute force methods.

Remediation:

The following setting is a recommend example policy. Alter these values to conform to your own organization's password policies.

Run the following command to install the `pam_pwquality` module:

```
# apt install libpam-pwquality
```

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password length to conform to site policy:

```
minlen = 14
```

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password complexity to conform to site policy:

Option 1

```
minclass = 4
```

Option 2

```
dcredit = -1

ucredit = -1

ocredit = -1

lcredit = -1
```

Edit the `/etc/pam.d/common-password` file to include `pam_pwquality.so` and to conform to site policy:

```
password requisite pam_pwquality.so retry=3
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: IA-5

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.4.2 Ensure lockout for failed password attempts is configured

Fail

Description:

Lock out users after *n* unsuccessful consecutive login attempts. The first sets of changes are made to the PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM.

- deny= `n` - `n` represents the number of failed attempts before the account is locked
- unlock_time= `n` - `n` represents the number of seconds before the account is unlocked
- audit - Will log the user name into the system log if the user is not found.
- silent - Don't print informative messages. Set the lockout number and unlock time in accordance with local site policy.

Rationale:

Locking out user IDs after `n` unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Remediation:

Edit the `/etc/pam.d/common-auth` file and add the auth line below:

```
auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900
```

Edit the `/etc/pam.d/common-account` file and add the account lines bellow:

```
account requisite pam_deny.so

account required pam_tally2.so
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AC-1, AC-2

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More >

Back to Summary

4.4.3 Ensure password reuse is limited

Fail

Description:

The `/etc/security/opasswd` file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

Rationale:

Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password.

Remediation:

NOTE: Pay special attention to the configuration. Incorrect configuration can cause system lock outs or unexpected behavior. This is example configuration. You configuration may differ based on previous changes to the files.

Edit the `/etc/pam.d/common-password` file to include:

- `password required pam_pwhistory.so remember=5`
- `use_authtok` on the `pam_unix.so` line

Example:

```
password required pam_pwhistory.so remember=5

password [success=1 default=ignore] pam_unix.so obscure sha512 use_authtok
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://manpages.ubuntu.com/manpages/focal/man8/pam_pwhistory.8.html
- **URL:** https://bugs.launchpad.net/ubuntu/+source/pam/+bug/1989731
- **URL:** NIST SP 800-53 Rev. 5: AC-2, IA-5

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More
>

Back to Summary

4.4.4 Ensure strong password hashing algorithm is configured

Pass

Description:

Hash functions behave as one-way functions by using mathematical operations that are extremely difficult and cumbersome to revert

When a user is created, the password is run through a one-way hashing algorithm before being stored. When the user logs in, the password sent is run through the same one-way hashing algorithm and compared to the hash connected with the provided username. If the hashed password and the stored hash match, the login is valid.

Rationale:

The `SHA512` hashing algorithm provides stronger hashing than previous available algorithms like `MD5` , thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

Remediation:

Note:

- Pay special attention to the configuration. Incorrect configuration can cause system lock outs.
- This is an example configuration. Your configuration may differ based on previous changes to the files.
- The encryption method on the password success line for `pam_unix.so` and the `ENCRYPT_METHOD` line in `/etc/login.defs` should match.

Edit the `/etc/pam.d/common-password` file and ensure that `sha512` is included and the `pam_unix.so` success line:

Example:

```
password [success=1 default=ignore] pam_unix.so obscure sha512 use_authtok
```

Edit `/etc/login.defs` and ensure that `ENCRYPT_METHOD` is set to `SHA512` .

```
ENCRYPT_METHOD SHA512
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: IA-5, SC-28

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More
>

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
>

Back to Summary

4.4.5 Ensure all current passwords uses the configured hashing algorithm

Manual

Description:

Currently used passwords with out of date hashing algorithms may pose a security risk to the system.

Rationale:

In use passwords should always match the configured hashing algorithm for the system.

Remediation:

If the administrator wish to force an immediate change on all users as per the output of the audit, execute:

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



{

UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)

awk -F: -v UID_MIN="${UID_MIN}" '( $3 >= UID_MIN && $1 != "nfsnobody" ) { print $1 }' /etc/passwd |
xargs -n 1 chage -d 0

}
```

NOTE: This could cause significant temporary CPU load on the system if a large number of users reset their passwords at the same time.

Impact:

If the administrator forces a password change, this could cause a large spike in CPU usage if a large number of users change their password during the same time.

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: IA-5, SC-28

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

4.5 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

4.5.1 Set Shadow Password Suite Parameters

While a majority of the password control parameters have been moved to PAM, some parameters are still available through the shadow password suite. Any changes made to `/etc/login.defs` will only be applied if the `usermod` command is used. If user IDs are added a different way, use the `chage` command to effect changes to individual user IDs.

4.5.1.1 Ensure minimum days between password changes is configured

Fail

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.

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>
```

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.5.1.2 Ensure password expiration is 365 days or less

Fail

Description:

The `PASS_MAX_DAYS` parameter in `/etc/login.defs` allows an administrator to force passwords to expire once they reach a defined age.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity. It is recommended that the `PASS_MAX_DAYS` parameter does not exceed `365` days and is greater than the value of `PASS_MIN_DAYS` .

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>
```

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://www.cisecurity.org/white-papers/cis-password-policy-guide/
- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.5.1.3 Ensure password expiration warning days is 7 or more

Pass

Description:

The `PASS_WARN_AGE` parameter in `/etc/login.defs` allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the `PASS_WARN_AGE` parameter be set to 7 or more days.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

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>
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.5.1.4 Ensure inactive password lock is 30 days or less

Fail

Description:

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

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>
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.5.1.5 Ensure all users last password change date is in the past

Pass

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.

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.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: IA-5

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.5.1.6 Ensure the number of changed characters in a new password is configured

Fail

Description:

The `pwqualitydifok` option sets the number of characters in a password that must not be present in the old password.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Remediation:

Edit or add the following line in `/etc/security/pwquality.conf` to a value of `2` or more:

```
difok = 2
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: IA-5

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.5.1.7 Ensure preventing the use of dictionary words for passwords is configured

Fail

Description:

The `pwqualitydictcheck` option sets whether to check for the words from the `cracklib` dictionary.

Rationale:

If the operating system allows the user to select passwords based on dictionary words, this increases the chances of password compromise by increasing the opportunity for successful guesses, and brute-force attacks.

Remediation:

Edit or add the following line in `/etc/security/pwquality.conf` to a value of `1` :

```
dictcheck = 1
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: IA-5

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

4.5.2 Ensure system accounts are secured

Pass

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.

Remediation:

Set the shell for any accounts returned by the audit to nologin:

```
# usermod -s $(which nologin) <user>
```

Lock any non root accounts returned by the audit:

```
# usermod -L <user>
```

The following script will:

- Set the shell for any accounts returned by the audit to nologin
- Lock any non root system accounts returned by the audit:

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



{
```

```
l_output="" l_output2=""

l_valid_shells="^($( awk -F\/ '$NF != "nologin" {print}' /etc/shells | sed -rn '/^\//{s,/,\\\\/,g;p}' |
paste -s -d '|' - ))$"

a_users=(); a_ulock=() # initialize arrays

while read -r l_user; do # change system accounts that have a valid login shell to nolog shell

echo -e " - System account \"$l_user\" has a valid logon shell, changing shell to \"$(which nologin)\""

usermod -s "$(which nologin)" "$l_user"

done < <(awk -v pat="$l_valid_shells" -F: '($1!~/(root|sync|shutdown|halt|^\+)/ && $3<'"$(awk
'/^\s*UID_MIN/{print $2}' /etc/login.defs)"' && $(NF) ~ pat) { print $1 }' /etc/passwd)

while read -r l_ulock; do # Lock system accounts that aren't locked

echo -e " - System account \"$l_ulock\" is not locked, locking account"

usermod -L "$l_ulock"

done < <(awk -v pat="$l_valid_shells" -F: '($1!~/(root|^\+)/ && $2!~/LK?/ && $3<'"$(awk
'/^\s*UID_MIN/{print $2}' /etc/login.defs)"' && $(NF) ~ pat) { print $1 }' /etc/passwd)

}
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

4.5.3 Ensure default group for the root account is GID 0

Pass

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.

Remediation:

Run the following command to set the `root` user default group to GID `0` :

```
# usermod -g 0 root
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

>

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
>

Back to Summary

4.5.4 Ensure default user umask is 027 or more restrictive

Fail

Description:

The user file-creation mode mask (`umask`) is use to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (rwxrwxrwx), and for any newly created file it is 0666 (rw-rw-rw-). The `umask` modifies the default Linux permissions by restricting (masking) these permissions. The `umask` is not simply subtracted, but is processed bitwise. Bits set in the `umask` are cleared in the resulting file mode.

`umask` *can be set with either* `octal` *or* `Symbolic` *values*

- `Octal` (Numeric) Value - Represented by either three or four digits. ie `umask 0027` or `umask 027` . If a four digit umask is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- `Symbolic` Value - Represented by a comma separated list for User `u` , group `g` , and world/other `o` . The permissions listed are not masked by `umask` . ie a `umask` set by `umask u=rwx,g=rx,o=` is the `Symbolic` equivalent of the `Octal``umask 027` . This `umask` would set a newly created directory with file mode `drwxr-x---` and a newly created file with file mode `rw-r-----` .

Setting the default `umask` :

- `pam_umask` module:
  - will set the umask according to the system default in `/etc/login.defs` and user settings, solving the problem of different `umask` settings with different shells, display managers, remote sessions etc.
  - `umask=<mask>` value in the `/etc/login.defs` file is interpreted as Octal
  - Setting `USERGROUPS_ENAB` to `yes` in `/etc/login.defs` (default):
    - will enable setting of the umask group bits to be the same as owner bits. (examples: 022 -> 002, 077 -> 007) for non-root users, if the uid is the same as gid, and username is the same as the primary group name
    - userdel will remove the user's group if it contains no more members, and useradd will create by default a group with the name of the user
- `System Wide Shell Configuration File:`
  - `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `.profile` , however this file is used to set an initial PATH or PS1 for all shell users of the system. *is only executed for interactive* `login` *shells, or shells executed with the --login parameter*
  - `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh` . It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
  - `/etc/bash.bashrc` - System wide version of `.bashrc` . `etc/bashrc` also invokes `/etc/profile.d/*.sh` if `non-login` shell, but redirects output to `/dev/null` if `non-interactive.` *Is only executed for* `interactive` *shells or if* `BASH_ENV` *is set to* `/etc/bash.bashrc`

User Shell Configuration Files:

- `~/.profile` - Is executed to configure your shell before the initial command prompt. *Is only read by login shells.*
- `~/.bashrc` - Is executed for interactive shells. *only read by a shell that's both interactive and non-login*

Rationale:

Setting a very secure default value for `umask` ensures that users make a conscious choice about their file permissions. A default `umask` setting of `077` causes files and directories created by users to not be readable by any other user on the system. A `umask` of `027` would make files and directories readable by users in the same Unix group, while a `umask` of `022` would make files readable by every user on the system.

Remediation:

Run the following command and remove or modify the `umask` of any returned files:

```
# grep -RPi '(^|^[^#]*)\s*umask\s+([0-7][0-7][01][0-7]\b|[0-7][0-7][0-7][0-6]\b|[0-7][01][0-7]\b|[0-7][0-7][0-6]\b|(u=[rwx]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+\b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(,o=[rwx]{0,3})?\b)' /etc/login.defs /etc/profile* /etc/bash.bashrc*
```

Follow **one** of the following methods to set the default user umask:

Edit `/etc/login.defs` and edit the `UMASK` and `USERGROUPS_ENAB` lines as follows:

```
UMASK 027
```

```
USERGROUPS_ENAB no
```

Edit `/etc/pam.d/common-session` and add or edit the following:

```
session optional pam_umask.so
```

OR

Configure umask in one of the following files:

- A file in the `/etc/profile.d/` directory ending in .sh
- `/etc/profile`
- `/etc/bash.bashrc`

Example: `/etc/profile.d/set_umask.sh`

```
umask 027
```

Note: this method only applies to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked.

Impact:

Setting `USERGROUPS_ENAB no` in `/etc/login.defs` may change the expected behavior of `useradd` and `userdel` .

Setting `USERGROUPS_ENAB yes` in `/etc/login.defs`

- `userdel` will remove the user's group if it contains no more members
- `useradd` will create by default a group with the name of the user.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** pam_umask(8)
- **URL:** NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

4.5.5 Ensure default user shell timeout is configured

Fail

Description:

`TMOUT` is an environmental setting that determines the timeout of a shell in seconds.

- TMOUT= *n* - Sets the shell timeout to *n* seconds. A setting of `TMOUT=0` disables timeout.
- readonly TMOUT- Sets the TMOUT environmental variable as readonly, preventing unwanted modification during run-time.
- export TMOUT - exports the TMOUT variable

`System Wide Shell Configuration Files:`

- `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `.bash_profile` , however this file is used to set an initial PATH or PS1 for all shell users of the system. **Is only executed for interactive *login* shells, or shells executed with the --login parameter.**
- `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh` . It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
- `/etc/bash.bashrc` - System wide version of `bash.bashrc` . `etc/bash.bashrc` also invokes `/etc/profile.d/*.sh` if *non-login* shell, but redirects output to `/dev/null` if *non-interactive*. **Is only executed for *interactive* shells or if** `BASH_ENV` **is set to** `/etc/bash.bashrc` .

Rationale:

Setting a timeout value reduces the window of opportunity for unauthorized user access to another user's shell session that has been left unattended. It also ends the inactive session and releases the resources associated with that session.

Remediation:

Review `/etc/bash.bashrc` , `/etc/profile` , and all files ending in `*.sh` in the `/etc/profile.d/` directory and remove or edit all `TMOUT=_n_` entries to follow local site policy.

`TMOUT` should:

- Be configured once, as multiple lines, or a single line, in **one and only one** of the following locations:
  - A file in the `/etc/profile.d/` directory ending in `.sh`
  - `/etc/profile`
  - `/etc/bash.bashrc`
- Not exceed `900`
- Not be equal to `0`

Multiple line example:

```
TMOUT=900

readonly TMOUT

export TMOUT
```

Single line example:

```
readonly TMOUT=900 ; export TMOUT
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AC-11

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

4.5.7 Ensure maximum number of same consecutive characters in a password is configured

Fail

Description:

The `pwqualitymaxrepeat` option sets the maximum number of allowed same consecutive characters in a new password.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Remediation:

Edit or add the following line in `/etc/security/pwquality.conf` to a value of `3` or less and not `0` :

```
maxrepeat = 3
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: IA-5

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

5 Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included in most distributions.

It is recommended that `rsyslog` be used for logging (with `logwatch` providing summarization) and `auditd` be used for auditing (with `aureport` providing summarization) to automatically monitor logs for intrusion attempts and other suspicious system behavior.

In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server via an encrypted connection. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized among systems and devices connected to the local network.

It is important that all logs described in this section be monitored on a regular basis and correlated to determine trends. A seemingly innocuous entry in one log could be more significant when compared to an entry in another log.

Note on log file permissions: There really isn't a "one size fits all" solution to the permissions on log files. Many sites utilize group permissions so that administrators who are in a defined security group, such as "wheel" do not have to elevate privileges to root in order to read log files. Also, if a third party log aggregation tool is used, it may need to have group permissions to read the log files, which is preferable to having it run setuid to root. Therefore, there are two remediation and audit steps for log file permissions. One is for systems that do not have a secured group method implemented that only permits root to read the log files (`root:root 600` *). The other is for sites that do have such a setup and are designated as* `root:securegrp 640` *where* `securegrp` *is the defined security group (in some cases* `wheel` *).*

5.1 Configure Logging

Logging services should be configured to prevent information leaks and to aggregate logs on a remote server so that they can be reviewed in the event of a system compromise. A centralized log server provides a single point of entry for further analysis, monitoring and filtering.

Security principals for logging

- Ensure transport layer security is implemented between the client and the log server.
- Ensure that logs are rotated as per the environment requirements.
- Ensure all locally generated logs have the appropriate permissions.
- Ensure all security logs are sent to a remote log server.
- Ensure the required events are logged.

What is covered

This section will cover the minimum best practices for the usage of **either**`rsyslog`**or**`journald` . The recommendations are written such that each is wholly independent of each other and **only one is implemented** .

- If your organization makes use of an enterprise wide logging system completely outside of `rsyslog` or `journald` , then the following recommendations does not directly apply. However, the principals of the recommendations should be followed regardless of what solution is

implemented. If the enterprise solution incorporates either of these tools, careful consideration should be given to the following recommendations to determine exactly what applies.
- Should your organization make use of both `rsyslog` and `journald` , take care how the recommendations may or may not apply to you.

What is not covered

- Enterprise logging systems not utilizing `rsyslog` or `journald` . As logging is very situational and dependant on the local environment, not everything can be covered here.
- Transport layer security should be applied to all remote logging functionality. Both `rsyslog` and `journald` supports secure transport and should be configured as such.
- The log server. There are a multitude of reasons for a centralized log server (and keeping a short period logging on the local system), but the log server is out of scope for these recommendations.

5.1.1 Configure journald

Included in the systemd suite is a journaling service called `systemd-journald.service` for the collection and storage of logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources such as:

- Classic RFC3164 BSD syslog via the /dev/log socket
- STDOUT/STDERR of programs via StandardOutput=journal + StandardError=journal in service files (both of which are default settings)
- Kernel log messages via the /dev/kmsg device node
- Audit records via the kernel's audit subsystem
- Structured log messages via journald's native protocol

Any changes made to the `systemd-journald` configuration will require a re-start of `systemd-journald`

5.1.1.1 Ensure journald is configured to send logs to a remote log host

5.1.1.1.1 Ensure systemd-journal-remote is installed

Pass

Description:

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Remediation:

Run the following command to install `systemd-journal-remote` :

```
# apt install systemd-journal-remote
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

5.1.1.1.2 Ensure systemd-journal-remote is configured

Manual

Description:

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Remediation:

Edit the `/etc/systemd/journal-upload.conf` file and ensure the following lines are set per your environment:

```
URL=192.168.50.42

ServerKeyFile=/etc/ssl/private/journal-upload.pem

ServerCertificateFile=/etc/ssl/certs/journal-upload.pem

TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Restart the service:

```
# systemctl restart systemd-journal-upload
```

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

5.1.1.1.3 Ensure systemd-journal-remote is enabled

Manual

Description:

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Remediation:

Run the following command to enable `systemd-journal-remote` :

```
# systemctl --now enable systemd-journal-upload.service
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-2, AU-12, CM-7, SI-5

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

5.1.1.1.4 Ensure journald is not configured to receive logs from a remote client

Pass

Description:

Journald supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

Note:

- The same package, `systemd-journal-remote` , is used for both sending logs to remote hosts and receiving incoming logs.
- With regards to receiving logs, there are two services; `systemd-journal-remote.socket` and `systemd-journal-remote.service` .

Rationale:

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside it's operational boundary.

Remediation:

Run the following command to disable `systemd-journal-remote.socket` :

```
# systemctl --now disable systemd-journal-remote.socket
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-2, AU-12, CM-6, CM-7

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

5.1.1.2 Ensure journald service is enabled

Pass

Description:

Ensure that the `systemd-journald` service is enabled to allow capturing of logging events.

Rationale:

If the `systemd-journald` service is not enabled to start on boot, the system will not capture logging events.

Remediation:

By default the `systemd-journald` service does not have an `[Install]` section and thus cannot be enabled / disabled. It is meant to be referenced as `Requires` or `Wants` by other unit files. As such, if the status of `systemd-journald` is not `static` , investigate why.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-2, AU-7 AU-12

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

5.1.1.3 Ensure journald is configured to compress large log files

Fail

Description:

The journald system includes the capability of compressing overly large files to avoid filling up the system with logs or making the logs unmanageably large.

Rationale:

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

Remediation:

Edit the `/etc/systemd/journald.conf` file or a file ending in .conf in /etc/systemd/journald.conf.d/ and add the following line:

```
Compress=yes
```

Restart the service:

```
# systemctl restart systemd-journald
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-4

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

5.1.1.4 Ensure journald is configured to write logfiles to persistent disk

Fail

Description:

Data from journald may be stored in volatile memory or persisted locally on the server. Logs in memory will be lost upon a system reboot. By persisting logs to local disk on the server they are protected from loss due to a reboot.

Rationale:

Writing log data to disk will provide the ability to forensically reconstruct events which may have impacted the operations or security of a system even after a system crash or reboot.

Remediation:

Edit the `/etc/systemd/journald.conf` file or a file ending in `.conf` in `/etc/systemd/journald.conf.d/` and add the following line:

```
Storage=persistent
```

Restart the service:

```
# systemctl restart systemd-journald
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-3, AU-12

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

5.1.1.5 Ensure journald is not configured to send logs to rsyslog

Manual

Description:

Data from `journald` should be kept in the confines of the service and not forwarded on to other services.

Rationale:

IF journald is the method for capturing logs, all logs of the system should be handled by journald and not forwarded to other logging mechanisms.

Remediation:

Edit the `/etc/systemd/journald.conf` file and files in `/etc/systemd/journald.conf.d/` and ensure that `ForwardToSyslog=yes` is removed.

Restart the service:

```
# systemctl restart systemd-journald
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-2, AU-6, AU-7, AU-12

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

5.1.1.6 Ensure journald log rotation is configured per site policy

Manual

Description:

Journald includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file `/etc/systemd/journald.conf` is the configuration file used to specify how logs generated by Journald should be rotated.

Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

Remediation:

Review `/etc/systemd/journald.conf` and verify logs are rotated according to site policy. The settings should be carefully understood as there are specific edge cases and prioritisation of parameters.

The specific parameters for log rotation are:

```
SystemMaxUse=

SystemKeepFree=

RuntimeMaxUse=

RuntimeKeepFree=

MaxFileSec=
```

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-2, AU-7, AU-12

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

5.1.1.7 Ensure journald default file permissions configured

Manual

Description:

Journald will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Remediation:

If the default configuration is not appropriate for the site specific requirements, copy `/usr/lib/tmpfiles.d/systemd.conf` to `/etc/tmpfiles.d/systemd.conf` and modify as required. Requirements is either `0640` or site policy if that is less restrictive.

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AC-3, AU-2, AU-12, MP-2, SI-5

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

5.1.2 Configure rsyslog

The `rsyslog` software package may be used instead of the default `journald` logging mechanism.

Note: This section only applies if `rsyslog` is the chosen method for client side logging. Do not apply this section if `journald` is used.

5.1.2.1 Ensure rsyslog is installed

Pass

Description:

The `rsyslog` software is recommended in environments where `journald` does not meet operation requirements.

Rationale:

The security enhancements of `rsyslog` such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

Remediation:

Run the following command to install `rsyslog` :

```
# apt install rsyslog
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-3, AU-12, SI-5

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

5.1.2.2 Ensure rsyslog service is enabled

Pass

Description:

Once the `rsyslog` package is installed, ensure that the service is enabled.

Rationale:

If the `rsyslog` service is not enabled to start on boot, the system will not capture logging events.

Remediation:

Run the following command to enable `rsyslog` :

```
# systemctl --now enable rsyslog
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-3, AU-12

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

5.1.2.3 Ensure journald is configured to send logs to rsyslog

Manual

Description:

Data from `journald` may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of `journald` logs, however, use of the RSyslog service provides a consistent means of log collection and export.

Rationale:

IF RSyslog is the preferred method for capturing logs, all logs of the system should be sent to it for further processing.

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
ForwardToSyslog=yes
```

Restart the service:

```
# systemctl restart rsyslog
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-9

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

5.1.2.4 Ensure rsyslog default file permissions are configured

Pass

Description:

RSyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Remediation:

Edit either `/etc/rsyslog.conf` or a dedicated `.conf` file in `/etc/rsyslog.d/` and set `$FileCreateMode` to `0640` or more restrictive:

```
$FileCreateMode 0640
```

Restart the service:

```
# systemctl restart rsyslog
```

Impact:

The systems global `umask` could override, but only making the file permissions stricter, what is configured in RSyslog with the `FileCreateMode` directive. RSyslog also has it's own `$umask` directive that can alter the intended file creation mode. In addition, consideration should be given to how `FileCreateMode` is used.

Thus it is critical to ensure that the intended file creation mode is not overridden with less restrictive settings in `/etc/rsyslog.conf` , `/etc/rsyslog.d/*conf` files and that `FileCreateMode` is set before any file is created.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the rsyslog.conf(5) man page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AC-3, AC-6, MP-2

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

5.1.2.5 Ensure logging is configured

Manual

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.).

Remediation:

Edit the following lines in the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files as appropriate for your environment.

NOTE: The below configuration is shown for example purposes only. Due care should be given to how the organization wish to store log data.

```
*.emerg :omusrmsg:*

auth,authpriv.* /var/log/secure

mail.* -/var/log/mail

mail.info -/var/log/mail.info

mail.warning -/var/log/mail.warn

mail.err /var/log/mail.err

cron.* /var/log/cron

*.=warning;*.=err -/var/log/warn

*.crit /var/log/warn

*.*;mail.none;news.none -/var/log/messages

local0,local1.* -/var/log/localmessages

local2,local3.* -/var/log/localmessages

local4,local5.* -/var/log/localmessages

local6,local7.* -/var/log/localmessages
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

Show Rule Result XML

References:

- **URL:** See the rsyslog.conf(5) man page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AU-2, AU-7, AU-12

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

5.1.2.6 Ensure rsyslog is configured to send logs to a remote log host

Manual

Description:

RSyslog supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and add the following line (where `loghost.example.com` is the name of your central log host). The `target` directive may either be a fully qualified domain name or an IP address.

```
*.* action(type="omfwd" target="192.168.2.100" port="514" protocol="tcp"

action.resumeRetryCount="100"

queue.type="LinkedList" queue.size="1000")
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** See the rsyslog.conf(5) man page for more information.
- **URL:** NIST SP 800-53 Rev. 5: AU-6

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

5.1.2.7 Ensure rsyslog is not configured to receive logs from a remote client

Pass

Description:

RSyslog supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

Rationale:

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside it's operational boundary.

Remediation:

Should there be any active log server configuration found in the auditing section, modify those file and remove the specific lines highlighted by the audit. Ensure none of the following entries are present in any of `/etc/rsyslog.conf` or `/etc/rsyslog.d/*.conf`.

Old format

```
$ModLoad imtcp

$InputTCPServerRun
```

New format

```
module(load="imtcp")

input(type="imtcp" port="514")
```

Restart the service:

```
# systemctl restart rsyslog
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-2, AU-6, AU-7, AU-12

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 8: Audit Log Management:** -- More

>

Back to Summary

5.1.3 Ensure all logfiles have appropriate access configured

Fail

Description:

Log files stored in `/var/log/` contain logged information from many services on the system and potentially from other logged hosts as well.

Rationale:

It is important that log files have the correct permissions to ensure that sensitive data is protected and that only the appropriate users / groups have access to them.

Remediation:

Run the following script to update permissions and ownership on files in `/var/log` .

Although the script is not destructive, ensure that the output is captured in the event that the remediation causes issues.

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



{

l_op2="" l_output2=""

l_uidmin="$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"

file_test_fix()

{

l_op2=""

l_fuser="root"

l_fgroup="root"

if [ $(( $l_mode & $perm_mask )) -gt 0 ]; then

l_op2="$l_op2\n - Mode: \"$l_mode\" should be \"$maxperm\" or more restrictive\n - Removing excess
permissions"

chmod "$l_rperms" "$l_fname"

fi

if [[ ! "$l_user" =~ $l_auser ]]; then

l_op2="$l_op2\n - Owned by: \"$l_user\" and should be owned by \"${l_auser//|/ or }\"\n - Changing
ownership to: \"$l_fuser\""

chown "$l_fuser" "$l_fname"

fi

if [[ ! "$l_group" =~ $l_agroup ]]; then

l_op2="$l_op2\n - Group owned by: \"$l_group\" and should be group owned by \"${l_agroup//|/ or }\"\n -
Changing group ownership to: \"$l_fgroup\""

chgrp "$l_fgroup" "$l_fname"

fi

[ -n "$l_op2" ] && l_output2="$l_output2\n - File: \"$l_fname\" is:$l_op2\n"

}

unset a_file && a_file=() # clear and initialize array

# Loop to create array with stat of files that could possibly fail one of the audits

while IFS= read -r -d $'\0' l_file; do
```

```
[ -e "$l_file" ] && a_file+=("$(stat -Lc '%n^%#a^%U^%u^%G^%g' "$l_file")")
done < <(find -L /var/log -type f \( -perm /0137 -o ! -user root -o ! -group root \) -print0)
while IFS="^" read -r l_fname l_mode l_user l_uid l_group l_gid; do
l_bname="$(basename "$l_fname")"
case "$l_bname" in
lastlog | lastlog.* | wtmp | wtmp.* | wtmp-* | btmp | btmp.* | btmp-* | README)
perm_mask='0113'
maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
l_rperms="ug-x,o-wx"
l_auser="root"
l_agroup="(root|utmp)"
file_test_fix
;;
secure | auth.log | syslog | messages)
perm_mask='0137'
maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
l_rperms="u-x,g-wx,o-rwx"
l_auser="(root|syslog)"
l_agroup="(root|adm)"
file_test_fix
;;
SSSD | sssd)
perm_mask='0117'
maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
l_rperms="ug-x,o-rwx"
l_auser="(root|SSSD)"
l_agroup="(root|SSSD)"
file_test_fix
;;
gdm | gdm3)
perm_mask='0117'
l_rperms="ug-x,o-rwx"
maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
l_auser="root"
l_agroup="(root|gdm|gdm3)"
file_test_fix
;;
*.journal | *.journal~)
perm_mask='0137'
maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
l_rperms="u-x,g-wx,o-rwx"
l_auser="root"
l_agroup="(root|systemd-journal)"
file_test_fix
```

```
;;

*)

perm_mask='0137'

maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"

l_rperms="u-x,g-wx,o-rwx"

l_auser="(root|syslog)"

l_agroup="(root|adm)"

if [ "$l_uid" -lt "$l_uidmin" ] && [ -z "$(awk -v grp="$l_group" -F: '$1==grp {print $4}' /etc/group)"
]; then

if [[ ! "$l_user" =~ $l_auser ]]; then

l_auser="(root|syslog|$l_user)"

fi

if [[ ! "$l_group" =~ $l_agroup ]]; then

l_tst=""

while l_out3="" read -r l_duid; do

[ "$l_duid" -ge "$l_uidmin" ] && l_tst=failed

done <<< "$(awk -F: '$4=='"$l_gid"' {print $3}' /etc/passwd)"

[ "$l_tst" != "failed" ] && l_agroup="(root|adm|$l_group)"

fi

fi

file_test_fix

;;

esac

done <<< "$(printf '%s\n' "${a_file[@]}")"

unset a_file # Clear array

# If all files passed, then we report no changes

if [ -z "$l_output2" ]; then

echo -e "- All files in \"/var/log/\" have appropriate permissions and ownership\n - No changes
required\n"

else

# print report of changes

echo -e "\n$l_output2"

fi

}
```

Note: You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.

If there are services that log to other locations, ensure that those log files have the appropriate access configured.

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

>

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
>

Back to Summary

5.2 Configure System Accounting (auditd)

The Linux Auditing System operates on a set of rules that collects certain types of system activity to facilitate incident investigation, detect unauthorized access or modification of data. By default events will be logged to `/var/log/audit/audit.log` , which can be configured in `/etc/audit/auditd.conf` .

The following types of audit rules can be specified:

- Control rules: Configuration of the auditing system.
- File system rules: Allow the auditing of access to a particular file or a directory. Also known as file watches.
- System call rules: Allow logging of system calls that any specified program makes.

Audit rules can be set:

- On the command line using the `auditctl` utility. These rules are not persistent across reboots.
- In `/etc/audit/audit.rules` . These rules have to be merged and loaded before they are active.

Notes:

- For 64 bit systems that have `arch` as a rule parameter, you will need two rules: one for 64 bit and one for 32 bit systems calls. For 32 bit systems, only one rule is needed.
- If the auditing system is configured to be locked (`-e 2`), a system reboot will be required in order to load any changes.
- Key names are optional on the rules and will not be used as a compliance auditing. The usage of key names is highly recommended as it facilitates organisation and searching, as such, all remediation steps will have key names supplied.
- It is best practice to store the rules, in number prepended files, in `/etc/audit/rules.d/` . Rules must end in a `.rules` suffix. This then requires the use of `augenrules` to merge all the rules into `/etc/audit/audit.rules` based on their their alphabetical (lexical) sort order. All benchmark recommendations follow this best practice for remediation, specifically using the prefix of `50` which is centre weighed if all rule sets make use of the number prepending naming convention.
- Your system may have been customized to change the default `UID_MIN` . All samples output uses `1000` , but this value will not be used in compliance auditing. To confirm the `UID_MIN` for your system, run the following command: `awk '/^\s*UID_MIN/{print $2}' /etc/login.defs`

Normalization

The Audit system normalizes some entries, so when you look at the sample output keep in mind that:

- With regards to users whose login UID is not set, the values `-1` / `unset` / `4294967295` are equivalent and normalized to `-1` .
- When comparing field types and both sides of the comparison is valid fields types, such as `euid!=uid` , then the auditing system may normalize such that the output is `uid!=euid` .
- Some parts of the rule may be rearranged whilst others are dependant on previous syntax. For example, the following two statements are the same:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F auid!=-1 -F key=user_emulation
```

and

```
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k user_emulation
```

Capacity planning

The recommendations in this section implement auditing policies that not only produces large quantities of logged data, but may also negatively impact system performance. Capacity planning is critical in order not to adversely impact production environments.

- Disk space. If a significantly large set of events are captured, additional on system or off system storage may need to be allocated. If the logs are not sent to a remote log server, ensure that log rotation is implemented else the disk will fill up and the system will halt. Even when logs are sent to a log server, ensure sufficient disk space to allow caching of logs in the case of temporary network outages.
- Disk IO. It is not just the amount of data collected that should be considered, but the rate at which logs are generated.
- CPU overhead. System call rules might incur considerable CPU overhead. Test the systems open/close syscalls per second with and without the rules to gauge the impact of the rules.

5.2.1 Ensure auditing is enabled

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

5.2.2 Configure Data Retention

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, auditd will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, check your site policy for audit storage requirements.

5.2.3 Configure auditd rules

The Audit system operates on a set of rules that define what is to be captured in the log files.

The following types of Audit rules can be specified:

- Control rules: Allow the Audit system's behavior and some of its configuration to be modified.
- File system rules: Allow the auditing of access to a particular file or a directory. (Also known as file watches)
- System call rules: Allow logging of system calls that any specified program makes.

Audit rules can be set:

- on the command line using the auditctl utility. Note that these rules are not persistent across reboots.
- in a file ending in `.rules` in the `/etc/audit/audit.d/` directory.

5.2.4 Configure auditd file access

Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events.

5.2.4.11 Ensure cryptographic mechanisms are used to protect the integrity of audit tools

Fail

Description:

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Attackers may replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

Audit tools should be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Remediation:

Add or update the following selection lines for to a file ending in `.conf` in the /etc/aide/aide.conf.d/ or to `/etc/aide/aide.conf` to protect the integrity of the audit tools:

```
# Audit Tools

/sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512

/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512

/sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512

/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512

/sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512

/sbin/augenrules p+i+n+u+g+s+b+acl+xattrs+sha512
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: AU-3

Back to Summary

6 System Maintenance

Recommendations in this section are intended as maintenance and are intended to be checked on a frequent basis to ensure system stability. Many recommendations do not have quick remediations and require investigation into the cause and best fix available and may indicate an attempted breach of system security.

6.1 System File Permissions

This section provides guidance on securing aspects of system files and directories.

6.1.1 Ensure permissions on /etc/passwd are configured

Pass

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.

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/passwd` :

```
# chmod u-x,go-wx /etc/passwd

# chown root:root /etc/passwd
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

6.1.2 Ensure permissions on /etc/passwd- are configured

Pass

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.

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/passwd-` :

```
# chmod u-x,go-wx /etc/passwd-

# chown root:root /etc/passwd-
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

6.1.3 Ensure permissions on /etc/group are configured

Pass

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.

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/group` :

```
# chmod u-x,go-wx /etc/group

# chown root:root /etc/group
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

6.1.4 Ensure permissions on /etc/group- are configured

Pass

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.

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/group-` :

```
# chmod u-x,go-wx /etc/group-

# chown root:root /etc/group-
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
  >

Back to Summary

6.1.5 Ensure permissions on /etc/shadow are configured

Pass

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.

Remediation:

Run **one** of the following commands to set ownership of `/etc/shadow` to `root` and group to either `root` or `shadow` :

```
# chown root:shadow /etc/shadow

-OR-

# chown root:root /etc/shadow
```

Run the following command to remove excess permissions form `/etc/shadow` :

```
# chmod u-x,g-wx,o-rwx /etc/shadow
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
  >

Back to Summary

6.1.6 Ensure permissions on /etc/shadow- are configured

Pass

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.

Remediation:

Run **one** of the following commands to set ownership of `/etc/shadow-` to `root` and group to either `root` or `shadow` :

```
# chown root:shadow /etc/shadow-

-OR-

# chown root:root /etc/shadow-
```

Run the following command to remove excess permissions form `/etc/shadow-` :

```
# chmod u-x,g-wx,o-rwx /etc/shadow-
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

6.1.7 Ensure permissions on /etc/gshadow are configured

Pass

Description:

The `/etc/gshadow` file is used to store the information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the `/etc/gshadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/gshadow` file (such as group administrators) could also be useful to subvert the group.

Remediation:

Run **one** of the following commands to set ownership of `/etc/gshadow` to `root` and group to either `root` or `shadow` :

```
# chown root:shadow /etc/gshadow

-OR-

# chown root:root /etc/gshadow
```

Run the following command to remove excess permissions form `/etc/gshadow` :

```
# chmod u-x,g-wx,o-rwx /etc/gshadow
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

6.1.8 Ensure permissions on /etc/gshadow- are configured

Pass

Description:

The `/etc/gshadow-` file is used to store backup information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

It is critical to ensure that the `/etc/gshadow-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Remediation:

Run **one** of the following commands to set ownership of `/etc/gshadow-` to `root` and group to either `root` or `shadow` :

```
# chown root:shadow /etc/gshadow-

-OR-

# chown root:root /etc/gshadow-
```

Run the following command to remove excess permissions form `/etc/gshadow-` :

```
# chmod u-x,g-wx,o-rwx /etc/gshadow-
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

6.1.9 Ensure permissions on /etc/shells are configured

Pass

Description:

`/etc/shells` is a text file which contains the full pathnames of valid login shells. This file is consulted by `chsh` and available to be queried by other programs.

Rationale:

It is critical to ensure that the `/etc/shells` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/shells` :

```
# chmod u-x,go-wx /etc/shells

# chown root:root /etc/shells
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

6.1.10 Ensure permissions on /etc/opasswd are configured

Fail

Description:

`/etc/security/opasswd` and it's backup `/etc/security/opasswd.old` hold user's previous passwords if `pam_unix` or `pam_pwhistory` is in use on the system

Rationale:

It is critical to ensure that `/etc/security/opasswd` is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/security/opasswd` and `/etc/security/opasswd.old` is they exist:

```
# [ -e "/etc/security/opasswd" ] && chmod u-x,go-rwx /etc/security/opasswd

# [ -e "/etc/security/opasswd" ] && chown root:root /etc/security/opasswd

# [ -e "/etc/security/opasswd.old" ] && chmod u-x,go-rwx /etc/security/opasswd.old

# [ -e "/etc/security/opasswd.old" ] && chown root:root /etc/security/opasswd.old
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
  >

Back to Summary

6.1.11 Ensure world writable files and directories are secured

Fail

Description:

World writable files are the least secure. Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity. See the `chmod(2)` man page for more information.

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

Rationale:

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

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

Remediation:

- World Writable Files:
  - It is recommended that write access is removed from `other` with the command (`chmod o-w <filename>`), but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.
- World Writable Directories:
  - Set the sticky bit on all world writable directories with the command (`chmod a+t <directory_name>`)

Run the following script to:

- Remove other write permission from any world writable files
- Add the sticky bit to all world writable directories

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



{

l_smask='01000'

a_path=(); a_arr=() # Initialize array

a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path "*/containerd/*" -a ! -path
"*/kubelet/pods/*" -a ! -path "/sys/kernel/security/apparmor/*" -a ! -path "/snap/*" -a ! -path
"/sys/fs/cgroup/memory/*")

while read -r l_bfs; do

a_path+=( -a ! -path ""$l_bfs"/*")

done < <(findmnt -Dkerno fstype,target | awk '$1 ~ /^\s*(nfs|proc|smb)/ {print $2}')

# Populate array with files

while IFS= read -r -d $'\0' l_file; do

[ -e "$l_file" ] && a_arr+=("$(stat -Lc '%n^%#a' "$l_file")")

done < <(find / \( "${a_path[@]}" \) \( -type f -o -type d \) -perm -0002 -print0 2>/dev/null)

while IFS="^" read -r l_fname l_mode; do # Test files in the array

if [ -f "$l_fname" ]; then # Remove excess permissions from WW files

echo -e " - File: \"$l_fname\" is mode: \"$l_mode\"\n - removing write permission on \"$l_fname\" from
\"other\""

chmod o-w "$l_fname"

fi

if [ -d "$l_fname" ]; then
```

```
if [ ! $(( $l_mode & $l_smask )) -gt 0 ]; then # Add sticky bit

echo -e " - Directory: \"$l_fname\" is mode: \"$l_mode\" and doesn't have the sticky bit set\n - Adding
the sticky bit"

chmod a+t "$l_fname"

fi

fi

done < <(printf '%s\n' "${a_arr[@]}")

unset a_path; unset a_arr # Remove array

}
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

6.1.12 Ensure no unowned or ungrouped files or directories exist

Fail

Description:

Administrators may delete users or groups from the system and neglect to remove all files and/or directories owned by those users or groups.

Rationale:

A new user or group who is assigned a deleted user's user ID or group ID may then end up "owning" a deleted user or group's files, and thus have more access on the system than was intended.

Remediation:

Remove or set ownership and group ownership of these files and/or directories to an active user on the system as appropriate.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

6.1.13 Ensure SUID and SGID files are reviewed

Manual

Description:

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID or SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SUID and SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different checksum than what from the package. This is an indication that the binary may have been replaced.

Remediation:

Ensure that no rogue SUID or SGID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5, AC-3, MP-2

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

6.2 Local User and Group Settings

This section provides guidance on securing aspects of the local users and groups.

Note: The recommendations in this section check local users and groups. Any users or groups from other sources such as LDAP will not be audited. In a domain environment similar checks should be performed against domain users and groups.

6.2.1 Ensure accounts in /etc/passwd use shadowed passwords

Pass

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.

Note:

- All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.
- A user account with an empty second field in `/etc/passwd` allows the account to be logged into by providing only the username.

Remediation:

Run the following command to set accounts to use shadowed passwords:

```
# sed -e 's/^\([a-zA-Z0-9_]*\):[^:]*:/\1:x:/' -i /etc/passwd
```

Investigate to determine if the account is logged in and what it is being used for, to determine if it needs to be forced off.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: IA-5

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

6.2.2 Ensure /etc/shadow password fields are not empty

Pass

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.

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.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: IA-5

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

6.2.3 Ensure all groups in /etc/passwd exist in /etc/group

Pass

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.

Remediation:

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Back to Summary

6.2.4 Ensure shadow group is empty

Pass

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.

Remediation:

Run the following command to remove all users from the shadow group

```
# sed -ri 's/(^shadow:[^:]*:[^:]*:)([^:]+$)/\1/' /etc/group
```

Change the primary group of any users with shadow as their primary group.

```
# usermod -g <primary group> <user>
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: IA-5

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
  >

Back to Summary

6.2.5 Ensure no duplicate UIDs exist

Pass

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.

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.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Back to Summary

6.2.6 Ensure no duplicate GIDs exist

Pass

Description:

Although the `groupadd` program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the `/etc/group` file and change the GID field.

Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

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.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Back to Summary

6.2.7 Ensure no duplicate user names exist

Pass

Description:

Although the `useradd` program will not let you create a duplicate user name, it is possible for an administrator to manually edit the `/etc/passwd` file and change the user name.

Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in `/etc/passwd` . For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.

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.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Back to Summary

6.2.8 Ensure no duplicate group names exist

Pass

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.

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.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Back to Summary

6.2.9 Ensure root PATH Integrity

Pass

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.

Remediation:

Correct or justify any items discovered in the Audit step.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Back to Summary

6.2.10 Ensure root is the only UID 0 account

Pass

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.

Remediation:

Remove any users other than `root` with UID `0` or assign them a new UID if appropriate.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Back to Summary

6.2.11 Ensure local interactive user home directories are configured

Fail

Description:

The user home directory is space defined for the particular user to set local environment variables and to store personal files. While the system administrator can establish secure permissions for users' home directories, the users can easily override these. Users can be defined in `/etc/passwd` without a home directory or with a home directory that does not actually exist.

Rationale:

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory. Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges. If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

Remediation:

If a local interactive users' home directory is undefined and/or doesn't exist, follow local site policy and perform one of the following:

- Lock the user account
- Remove the user from the system
- create a directory for the user. If undefined, edit `/etc/passwd` and add the absolute path to the directory to the last field of the user.

Run the following script to:

- Remove excessive permissions from local interactive users home directories
- Update the home directory's owner

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



{

l_output2=""

l_valid_shells="^($( awk -F\/ '$NF != "nologin" {print}' /etc/shells | sed -rn '/^\//{s,/,\\\\/,g;p}' |
paste -s -d '|' - ))$"

unset a_uarr && a_uarr=() # Clear and initialize array

while read -r l_epu l_eph; do # Populate array with users and user home location

a_uarr+=("$l_epu $l_eph")

done <<< "$(awk -v pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }' /etc/passwd)"

l_asize="${#a_uarr[@]}" # Here if we want to look at number of users before proceeding

[ "$l_asize " -gt "10000" ] && echo -e "\n ** INFO **\n - \"$l_asize\" Local interactive users found on
the system\n - This may be a long running process\n"

while read -r l_user l_home; do

if [ -d "$l_home" ]; then

l_mask='0027'

l_max="$( printf '%o' $(( 0777 & ~$l_mask)) )"

while read -r l_own l_mode; do
```

```
if [ "$l_user" != "$l_own" ]; then

l_output2="$l_output2\n - User: \"$l_user\" Home \"$l_home\" is owned by: \"$l_own\"\n - changing
ownership to: \"$l_user\"\n"

chown "$l_user" "$l_home"

fi

if [ $(( $l_mode & $l_mask )) -gt 0 ]; then

l_output2="$l_output2\n - User: \"$l_user\" Home \"$l_home\" is mode: \"$l_mode\" should be mode:
\"$l_max\" or more restrictive\n - removing excess permissions\n"

chmod g-w,o-rwx "$l_home"

fi

done <<< "$(stat -Lc '%U %#a' "$l_home")"

else

l_output2="$l_output2\n - User: \"$l_user\" Home \"$l_home\" Doesn't exist\n - Please create a home in
accordance with local site policy"

fi

done <<< "$(printf '%s\n' "${a_uarr[@]}")"

if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass

echo -e " - No modification needed to local interactive users home directories"

else

echo -e "\n$l_output2"

fi

}
```

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

6.2.12 Ensure local interactive user dot files access is configured

Fail

Description:

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

- `.forward` file specifies an email address to forward the user's mail to.
- `.rhost` file provides the "remote authentication" database for the rcp, rlogin, and rsh commands and the rcmd() function. These files bypass the standard password-based user authentication mechanism. They specify remote hosts and users that are considered trusted (i.e. are allowed to access the local system without supplying a password)
- `.netrc` file contains data for logging into a remote host or passing authentication to an API.
- `.bash_history` file keeps track of the user's last 500 commands.

Rationale:

User configuration files with excessive or incorrect access may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.

The following script will:

- remove excessive permissions on `dot` files within interactive users' home directories
- change ownership of `dot` files within interactive users' home directories to the user
- change group ownership of `dot` files within interactive users' home directories to the user's primary group
- list `.forward` and `.rhost` files to be investigated and manually deleted

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



{

l_valid_shells="^($( awk -F\/ '$NF != "nologin" {print}' /etc/shells | sed -rn '/^\//{s,/,\\\\/,g;p}' |
paste -s -d '|' - ))$"

unset a_uarr && a_uarr=() # Clear and initialize array

while read -r l_epu l_eph; do # Populate array with users and user home location

[[ -n "$l_epu" && -n "$l_eph" ]] && a_uarr+=("$l_epu $l_eph")

done <<< "$(awk -v pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }' /etc/passwd)"

l_asize="${#a_uarr[@]}" # Here if we want to look at number of users before proceeding

l_maxsize="1000" # Maximum number of local interactive users before warning (Default 1,000)

[ "$l_asize " -gt "$l_maxsize" ] && echo -e "\n ** INFO **\n - \"$l_asize\" Local interactive users
found on the system\n - This may be a long running check\n"

file_access_fix()

{

l_facout2=""

l_max="$( printf '%o' $(( 0777 & ~$l_mask)) )"

if [ $(( $l_mode & $l_mask )) -gt 0 ]; then

echo -e " - File: \"$l_hdfile\" is mode: \"$l_mode\" and should be mode: \"$l_max\" or more
restrictive\n - Changing to mode \"$l_max\""

chmod "$l_chp" "$l_hdfile"

fi

if [[ ! "$l_owner" =~ ($l_user) ]]; then

echo -e " - File: \"$l_hdfile\" owned by: \"$l_owner\" and should be owned by \"${l_user//|/ or }\"\n -
Changing ownership to \"$l_user\""

chown "$l_user" "$l_hdfile"

fi

if [[ ! "$l_gowner" =~ ($l_group) ]]; then

echo -e " - File: \"$l_hdfile\" group owned by: \"$l_gowner\" and should be group owned by
\"${l_group//|/ or }\"\n - Changing group ownership to \"$l_group\""

chgrp "$l_group" "$l_hdfile"

fi

}

while read -r l_user l_home; do

if [ -d "$l_home" ]; then

echo -e "\n - Checking user: \"$l_user\" home directory: \"$l_home\""

l_group="$(id -gn "$l_user" | xargs)"

l_group="${l_group// /|}"

while IFS= read -r -d $'\0' l_hdfile; do
```

```
while read -r l_mode l_owner l_gowner; do
case "$(basename "$l_hdfile")" in
.forward | .rhost )
echo -e " - File: \"$l_hdfile\" exists\n - Please investigate and manually delete \"$l_hdfile\""
;;
.netrc )
l_mask='0177'
l_chp="u-x,go-rwx"
file_access_fix ;;
.bash_history )
l_mask='0177'
l_chp="u-x,go-rwx"
file_access_fix ;;
* )
l_mask='0133'
l_chp="u-x,go-wx"
file_access_fix ;;
esac
done <<< "$(stat -Lc '%#a %U %G' "$l_hdfile")"
done < <(find "$l_home" -xdev -type f -name '.*' -print0)
fi
done <<< "$(printf '%s\n' "${a_uarr[@]}")"
unset a_uarr # Remove array
}
```

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More >

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

⇧