Security Configuration Assessment Report for mgs-650

CIS-CAT Host IP Address: 127.0.1.1

CIS Ubuntu Linux 16.04 LTS Benchmark v1.0.0

Level 1 - Server
Saturday, December 3 2022 17:25:17

Report generated by the Center for Internet Security's Configuration Assessment Tool (CIS-CAT) v3.0.43.
For further information, please visit The Center for Internet Security or send an e-mail to feedback@cisecurity.org.
Copyright ©2022, The Center for Internet Security

Summary

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
1 Initial Setup	**14**	**14**	**0**	**1**	**14.0**	**29.0**	**48%**
1.1 Filesystem Configuration	9	9	0	1	9.0	19.0	47%
1.1.1 Disable unused filesystems	0	8	0	0	0.0	8.0	0%
1.2 Configure Software Updates	0	0	0	0	0.0	0.0	0%
1.3 Filesystem Integrity Checking	0	2	0	0	0.0	2.0	0%
1.4 Secure Boot Settings	0	2	0	0	0.0	2.0	0%
1.5 Additional Process Hardening	2	1	0	0	2.0	3.0	67%
1.6 Mandatory Access Control	0	0	0	0	0.0	0.0	0%
1.6.1 Configure SELinux	0	0	0	0	0.0	0.0	0%
1.6.2 Configure AppArmor	0	0	0	0	0.0	0.0	0%
1.7 Warning Banners	3	0	0	0	3.0	3.0	100%
1.7.1 Command Line Warning Banners	2	0	0	0	2.0	2.0	100%
2 Services	**26**	**7**	**0**	**0**	**26.0**	**33.0**	**79%**
2.1 inetd Services	9	1	0	0	9.0	10.0	90%
2.2 Special Purpose Services	13	5	0	0	13.0	18.0	72%
2.2.1 Time Synchronization	2	0	0	0	2.0	2.0	100%
2.3 Service Clients	4	1	0	0	4.0	5.0	80%
3 Network Configuration	**12**	**7**	**0**	**0**	**12.0**	**19.0**	**63%**
3.1 Network Parameters (Host Only)	1	1	0	0	1.0	2.0	50%
3.2 Network Parameters (Host and Router)	5	3	0	0	5.0	8.0	62%
3.3 IPv6	0	0	0	0	0.0	0.0	0%
3.4 TCP Wrappers	4	1	0	0	4.0	5.0	80%
3.5 Uncommon Network Protocols	0	0	0	0	0.0	0.0	0%
3.6 Firewall Configuration	2	2	0	0	2.0	4.0	50%
4 Logging and Auditing	**5**	**2**	**0**	**0**	**5.0**	**7.0**	**71%**
4.1 Configure System Accounting (auditd)	0	0	0	0	0.0	0.0	0%
4.1.1 Configure Data Retention	0	0	0	0	0.0	0.0	0%
4.2 Configure Logging	5	2	0	0	5.0	7.0	71%
4.2.1 Configure rsyslog	2	1	0	0	2.0	3.0	67%
4.2.2 Configure syslog-ng	2	0	0	0	2.0	2.0	100%
5 Access, Authentication and Authorization	**9**	**25**	**0**	**0**	**9.0**	**34.0**	**26%**
5.1 Configure cron	1	7	0	0	1.0	8.0	12%
5.2 SSH Server Configuration	5	10	0	0	5.0	15.0	33%
5.3 Configure PAM	1	2	0	0	1.0	3.0	33%
5.4 User Accounts and Environment	2	5	0	0	2.0	7.0	29%
5.4.1 Set Shadow Password Suite Parameters	1	3	0	0	1.0	4.0	25%
6 System Maintenance	**24**	**4**	**0**	**3**	**24.0**	**31.0**	**77%**
6.1 System File Permissions	8	0	0	3	8.0	11.0	73%
6.2 User and Group Settings	16	4	0	0	16.0	20.0	80%
Total	**90**	**59**	**0**	**4**	**90.0**	**153.0**	**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.
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.

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

⇧

Assessment Results

Display Failures Only

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
1.0	1.1.1.6 Ensure mounting of squashfs filesystems is disabled	Fail
1.0	1.1.1.7 Ensure mounting of udf filesystems is disabled	Fail
1.0	1.1.1.8 Ensure mounting of FAT filesystems is disabled	Fail
1.0	1.1.3 Ensure nodev option set on /tmp partition	Pass
1.0	1.1.4 Ensure nosuid option set on /tmp partition	Pass
1.0	1.1.7 Ensure nodev option set on /var/tmp partition	Pass
1.0	1.1.8 Ensure nosuid option set on /var/tmp partition	Pass
1.0	1.1.9 Ensure noexec option set on /var/tmp partition	Pass
1.0	1.1.13 Ensure nodev option set on /home partition	Pass
1.0	1.1.14 Ensure nodev option set on /dev/shm partitiov	Pass
1.0	1.1.15 Ensure nosuid option set on /dev/shm partitionrun	Pass
1.0	1.1.16 Ensure noexec option set on /dev/shm partition	Fail
1.0	1.1.20 Ensure sticky bit is set on all world-writable directories	Unknown
1.0	1.1.21 Disable Automounting	Pass
1.2 Configure Software Updates		
1.3 Filesystem Integrity Checking		
1.0	1.3.1 Ensure AIDE is installed	Fail
1.0	1.3.2 Ensure filesystem integrity is regularly checked	Fail
1.4 Secure Boot Settings		
1.0	1.4.1 Ensure permissions on bootloader config are configured	Fail
1.0	1.4.2 Ensure bootloader password is set	Fail
1.5 Additional Process Hardening		
1.0	1.5.1 Ensure core dumps are restricted	Fail
	1.5.2 Ensure XD/NX support is enabled	Informational

w	Benchmark Item	Result
1.0	1.5.3 Ensure address space layout randomization (ASLR) is enabled	Pass
1.0	1.5.4 Ensure prelink is disabled	Pass
	1.6 Mandatory Access Control	
	1.6.1 Configure SELinux	
	1.6.2 Configure AppArmor	
	1.7 Warning Banners	
	1.7.1 Command Line Warning Banners	
1.0	1.7.1.1 Ensure message of the day is configured properly	Pass
	1.7.1.2 Ensure local login warning banner is configured properly	Informational
	1.7.1.3 Ensure remote login warning banner is configured properly	Informational
	1.7.1.4 Ensure permissions on /etc/motd are configured	Informational
1.0	1.7.1.5 Ensure permissions on /etc/issue are configured	Pass
	1.7.1.6 Ensure permissions on /etc/issue.net are configured	Informational
1.0	1.7.2 Ensure GDM login banner is configured	Pass
	2 Services	
	2.1 inetd Services	
1.0	2.1.1 Ensure chargen services are not enabled	Pass
1.0	2.1.2 Ensure daytime services are not enabled	Pass
1.0	2.1.3 Ensure discard services are not enabled	Pass
1.0	2.1.4 Ensure echo services are not enabled	Pass
1.0	2.1.5 Ensure time services are not enabled	Pass
1.0	2.1.6 Ensure rsh server is not enabled	Pass
1.0	2.1.7 Ensure talk server is not enabled	Pass
1.0	2.1.8 Ensure telnet server is not enabled	Pass
1.0	2.1.9 Ensure tftp server is not enabled	Pass
1.0	2.1.10 Ensure xinetd is not enabled	Fail
	2.2 Special Purpose Services	
	2.2.1 Time Synchronization	
	2.2.1.1 Ensure time synchronization is in use	Informational
1.0	2.2.1.2 Ensure ntp is configured	Pass
1.0	2.2.1.3 Ensure chrony is configured	Pass
1.0	2.2.2 Ensure X Window System is not installed	Fail
1.0	2.2.3 Ensure Avahi Server is not enabled	Fail
1.0	2.2.4 Ensure CUPS is not enabled	Fail
1.0	2.2.5 Ensure DHCP Server is not enabled	Pass
1.0	2.2.6 Ensure LDAP server is not enabled	Pass
1.0	2.2.7 Ensure NFS and RPC are not enabled	Pass
1.0	2.2.8 Ensure DNS Server is not enabled	Pass
1.0	2.2.9 Ensure FTP Server is not enabled	Fail
1.0	2.2.10 Ensure HTTP server is not enabled	Fail
1.0	2.2.11 Ensure IMAP and POP3 server is not enabled	Pass
1.0	2.2.12 Ensure Samba is not enabled	Pass
1.0	2.2.13 Ensure HTTP Proxy Server is not enabled	Pass
1.0	2.2.14 Ensure SNMP Server is not enabled	Pass
1.0	2.2.15 Ensure mail transfer agent is configured for local-only mode	Pass
1.0	2.2.16 Ensure rsync service is not enabled	Pass
1.0	2.2.17 Ensure NIS Server is not enabled	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
	3 Network Configuration	
	3.1 Network Parameters (Host Only)	

w	Benchmark Item	Result
1.0	3.1.1 Ensure IP forwarding is disabled	Pass
1.0	3.1.2 Ensure packet redirect sending is disabled	Fail
	3.2 Network Parameters (Host and Router)	
1.0	3.2.1 Ensure source routed packets are not accepted	Pass
1.0	3.2.2 Ensure ICMP redirects are not accepted	Pass
1.0	3.2.3 Ensure secure ICMP redirects are not accepted	Fail
1.0	3.2.4 Ensure suspicious packets are logged	Fail
1.0	3.2.5 Ensure broadcast ICMP requests are ignored	Pass
1.0	3.2.6 Ensure bogus ICMP responses are ignored	Pass
1.0	3.2.7 Ensure Reverse Path Filtering is enabled	Pass
1.0	3.2.8 Ensure TCP SYN Cookies is enabled	Fail
	3.3 IPv6	
	3.3.1 Ensure IPv6 router advertisements are not accepted	Informational
	3.3.2 Ensure IPv6 redirects are not accepted	Informational
	3.3.3 Ensure IPv6 is disabled	Informational
	3.4 TCP Wrappers	
1.0	3.4.1 Ensure TCP Wrappers is installed	Pass
1.0	3.4.2 Ensure /etc/hosts.allow is configured	Pass
1.0	3.4.3 Ensure /etc/hosts.deny is configured	Fail
1.0	3.4.4 Ensure permissions on /etc/hosts.allow are configured	Pass
1.0	3.4.5 Ensure permissions on /etc/hosts.deny are 644	Pass
	3.5 Uncommon Network Protocols	
	3.5.1 Ensure DCCP is disabled	Informational
	3.5.2 Ensure SCTP is disabled	Informational
	3.5.3 Ensure RDS is disabled	Informational
	3.5.4 Ensure TIPC is disabled	Informational
	3.6 Firewall Configuration	
1.0	3.6.1 Ensure iptables is installed	Pass
1.0	3.6.2 Ensure default deny firewall policy	Pass
1.0	3.6.3 Ensure loopback traffic is configured	Fail
1.0	3.6.5 Ensure firewall rules exist for all open ports	Fail
	4 Logging and Auditing	
	4.1 Configure System Accounting (auditd)	
	4.1.1 Configure Data Retention	
	4.2 Configure Logging	
	4.2.1 Configure rsyslog	
1.0	4.2.1.1 Ensure rsyslog Service is enabled	Pass
1.0	4.2.1.3 Ensure rsyslog default file permissions configured	Pass
1.0	4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host	Fail
	4.2.2 Configure syslog-ng	
1.0	4.2.2.1 Ensure syslog-ng service is enabled	Pass
1.0	4.2.2.3 Ensure syslog-ng default file permissions configured	Pass
1.0	4.2.3 Ensure rsyslog or syslog-ng is installed	Pass
1.0	4.2.4 Ensure permissions on all logfiles are configured	Fail
	5 Access, Authentication and Authorization	
	5.1 Configure cron	
1.0	5.1.1 Ensure cron daemon is enabled	Pass
1.0	5.1.2 Ensure permissions on /etc/crontab are configured	Fail
1.0	5.1.3 Ensure permissions on /etc/cron.hourly are configured	Fail
1.0	5.1.4 Ensure permissions on /etc/cron.daily are configured	Fail
1.0	5.1.5 Ensure permissions on /etc/cron.weekly are configured	Fail
1.0	5.1.6 Ensure permissions on /etc/cron.monthly are configured	Fail
1.0	5.1.7 Ensure permissions on /etc/cron.d are configured	Fail
1.0	5.1.8 Ensure at/cron is restricted to authorized users	Fail
	5.2 SSH Server Configuration	
1.0	5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured	Fail

w	Benchmark Item	Result
1.0	5.2.2 Ensure SSH Protocol is set to 2	Pass
1.0	5.2.3 Ensure SSH LogLevel is set to INFO	Pass
1.0	5.2.4 Ensure SSH X11 forwarding is disabled	Fail
1.0	5.2.5 Ensure SSH MaxAuthTries is set to 4 or less	Fail
1.0	5.2.6 Ensure SSH IgnoreRhosts is enabled	Pass
1.0	5.2.7 Ensure SSH HostbasedAuthentication is disabled	Pass
1.0	5.2.8 Ensure SSH root login is disabled	Fail
1.0	5.2.9 Ensure SSH PermitEmptyPasswords is disabled	Pass
1.0	5.2.10 Ensure SSH PermitUserEnvironment is disabled	Fail
1.0	5.2.11 Ensure only approved MAC algorithms are used	Fail
1.0	5.2.12 Ensure SSH Idle Timeout Interval is configured	Fail
1.0	5.2.13 Ensure SSH LoginGraceTime is set to one minute or less	Fail
1.0	5.2.14 Ensure SSH access is limited	Fail
1.0	5.2.15 Ensure SSH warning banner is configured	Fail
	5.3 Configure PAM	
1.0	5.3.1 Ensure password creation requirements are configured	Fail
1.0	5.3.3 Ensure password reuse is limited	Fail
1.0	5.3.4 Ensure password hashing algorithm is SHA-512	Pass
	5.4 User Accounts and Environment	
	5.4.1 Set Shadow Password Suite Parameters	
1.0	5.4.1.1 Ensure password expiration is 90 days or less	Fail
1.0	5.4.1.2 Ensure minimum days between password changes is 7 or more	Fail
1.0	5.4.1.3 Ensure password expiration warning days is 7 or more	Pass
1.0	5.4.1.4 Ensure inactive password lock is 30 days or less	Fail
1.0	5.4.2 Ensure system accounts are non-login	Fail
1.0	5.4.3 Ensure default group for the root account is GID 0	Pass
1.0	5.4.4 Ensure default user umask is 027 or more restrictive	Fail
1.0	5.6 Ensure access to the su command is restricted	Fail
	6 System Maintenance	
	6.1 System File Permissions	
1.0	6.1.2 Ensure permissions on /etc/passwd are configured	Pass
1.0	6.1.3 Ensure permissions on /etc/shadow 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/gshadow are configured	Pass
1.0	6.1.6 Ensure permissions on /etc/passwd- are configured	Pass
1.0	6.1.7 Ensure permissions on /etc/shadow- are configured	Pass
1.0	6.1.8 Ensure permissions on /etc/group- are configured	Pass
1.0	6.1.9 Ensure permissions on /etc/gshadow- are configured	Pass
1.0	6.1.10 Ensure no world writable files exist	Unknown
1.0	6.1.11 Ensure no unowned files or directories exist	Unknown
1.0	6.1.12 Ensure no ungrouped files or directories exist	Unknown
	6.2 User and Group Settings	
1.0	6.2.1 Ensure password fields are not empty	Fail
1.0	6.2.2 Ensure no legacy "+" entries exist in /etc/passwd	Pass
1.0	6.2.3 Ensure no legacy "+" entries exist in /etc/shadow	Pass
1.0	6.2.4 Ensure no legacy "+" entries exist in /etc/group	Pass
1.0	6.2.5 Ensure root is the only UID 0 account	Pass
1.0	6.2.6 Ensure root PATH Integrity	Fail
1.0	6.2.7 Ensure all users' home directories exist	Fail
1.0	6.2.8 Ensure users' home directories permissions are 750 or more restrictive	Fail
1.0	6.2.9 Ensure users own their home directories	Pass
1.0	6.2.10 Ensure users' dot files are not group or world writable	Pass
1.0	6.2.11 Ensure no users have .forward files	Pass
1.0	6.2.12 Ensure no users have .netrc files	Pass

w	Benchmark Item	Result
1.0	6.2.13 Ensure users' .netrc Files are not group or world accessible	Pass
1.0	6.2.14 Ensure no users have .rhosts files	Pass
1.0	6.2.15 Ensure all groups in /etc/passwd exist in /etc/group	Pass
1.0	6.2.16 Ensure no duplicate UIDs exist	Pass
1.0	6.2.17 Ensure no duplicate GIDs exist	Pass
1.0	6.2.18 Ensure no duplicate user names exist	Pass
1.0	6.2.19 Ensure no duplicate group names exist	Pass
1.0	6.2.20 Ensure shadow group is empty	Pass

⇧

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

1.1.1 Disable unused filesystems

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

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

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

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

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install cramfs /bin/true
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure kernel module cramfs is not loadable -- Less

Check:	At Least One Must Pass
Command:	modprobe -n -v cramfs
Line Selection:	.+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/drivers/mtd/mtd.ko
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/fs/cramfs/cramfs.ko

Ensure kernel module cramfs is not loaded -- 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:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install freevxfs /bin/true
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure kernel module freevxfs is not loadable -- Less

Check:	At Least One Must Pass
Command:	modprobe -n -v freevxfs
Line Selection:	.+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/fs/freevxfs/freevxfs.ko

Ensure kernel module freevxfs is not loaded -- 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:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install jffs2 /bin/true
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure kernel module jffs2 is not loadable -- Less

Check:	At Least One Must Pass
Command:	modprobe -n -v jffs2
Line Selection:	.+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/drivers/mtd/mtd.ko
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/fs/jffs2/jffs2.ko

Ensure kernel module jffs2 is not loaded -- 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:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install hfs /bin/true
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure kernel module hfs is not loadable -- Less

Check:	At Least One Must Pass
Command:	modprobe -n -v hfs
Line Selection:	.+

CIS-CAT Expected (At least one of)... CIS-CAT Collected...

the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**

Ensure kernel module hfs is not loaded -- Less

Check:	None May Pass
Command:	lsmod
Line Selection:	.+

CIS-CAT Expected (At least one of)... CIS-CAT Collected...

the *Std. Output* matches the regular Module Size Used by

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:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install hfsplus /bin/true
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure kernel module hfsplus is not loaded -- Less

Check:	None May Pass
Command:	lsmod
Line Selection:	.+

CIS-CAT Expected	CIS-CAT Collected...
(At least one of)... the *Std. Output* matches the regular	Module Size Used by

Ensure kernel module hfsplus is not loadable -- Less

Check:	At Least One Must Pass
Command:	modprobe -n -v hfsplus
Line Selection:	.+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	

Back to Summary

1.1.1.6 Ensure mounting of squashfs filesystems is disabled

Fail

Description:

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

Rationale:

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

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install squashfs /bin/true
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure kernel module squashfs is not loadable -- Less

Check:	At Least One Must Pass
Command:	modprobe -n -v squashfs
Line Selection:	.+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	

Ensure kernel module squashfs is not loaded -- More

Back to Summary

1.1.1.7 Ensure mounting of udf filesystems is disabled

Fail

Description:

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

to support writing DVDs and newer optical disc formats.

Rationale:

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

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install udf /bin/true
```

Assessment:

All of the following tests or sub-groups must pass:
Ensure kernel module udf is not loaded -- More
Ensure kernel module udf is not loadable -- Less

Check:	At Least One Must Pass
Command:	modprobe -n -v udf
Line Selection:	.+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/lib/crc-itu-t.ko
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/fs/udf/udf.ko

Back to Summary

1.1.1.8 Ensure mounting of FAT filesystems is disabled

Fail

Description:

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

Rationale:

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

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install vfat /bin/true
```

Impact:

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

Assessment:

All of the following tests or sub-groups must pass:
Ensure kernel module vfat is not loadable -- Less

Check:	At Least One Must Pass
Command:	modprobe -n -v vfat
Line Selection:	.+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	

Ensure kernel module vfat is not loaded -- More

Back to Summary

1.1.3 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 attempt to 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. See the `fstab(5)` manual page for more information.

Run the following command to remount `/tmp`:

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

Assessment:

Ensure partition at /tmp may exists and all have at least one partition option equals 'nodev' (string) -- More

Back to Summary

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

Run the following command to remount `/tmp`:

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

Assessment:

Ensure partition at /tmp may exists and all have at least one partition option equals 'nosuid' (string) -- More

Back to Summary

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

Remediation:

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

Run the following command to remount /var/tmp:

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

Assessment:

Ensure partition at /var/tmp may exists and all have at least one partition option equals 'nodev' (string) -- More

Back to Summary

1.1.8 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:

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

Run the following command to remount /var/tmp:

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

Assessment:

Ensure partition at /var/tmp may exists and all have at least one partition option equals 'nosuid' (string) -- More

Back to Summary

1.1.9 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:

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

Run the following command to remount /var/tmp:

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

Assessment:

Ensure partition at /var/tmp may exists and all have at least one partition option equals 'noexec' (string) -- More

Back to Summary

1.1.13 Ensure nodev option set on /home partition

Pass

Description:

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

Rationale:

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

Remediation:

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

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

Assessment:

Ensure partition at /home may exists and all have at least one partition option equals 'nodev' (string) -- More

Back to Summary

1.1.14 Ensure nodev option set on /dev/shm partitiov

Pass

Description:

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

Rationale:

Since the `/run/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.

Run the following command to remount `/dev/shm`:

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

Assessment:

Ensure partition at /dev/shm may exists and all have at least one partition option equals 'nodev' (string) -- More

Back to Summary

1.1.15 Ensure nosuid option set on /dev/shm partitionrun

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.

Run the following command to remount `/dev/shm`:

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

Assessment:

Ensure partition at /dev/shm may exists and all have at least one partition option equals 'nosuid' (string) -- More

Back to Summary

1.1.16 Ensure noexec option set on /dev/shm partition

Fail

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

Run the following command to remount `/dev/shm`:

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

Assessment:

Ensure partition at /dev/shm may exists and all have at least one partition option equals 'noexec' (string) -- Less

Check:	All Must Pass	
Mount Point:	/dev/shm	
CIS-CAT Expected (At least one of)...		CIS-CAT Collected...
the *Mount Options* to be set to **noexec**		rw
the *Mount Options* to be set to **noexec**		nosuid
the *Mount Options* to be set to **noexec**		nodev

Back to Summary

1.1.20 Ensure sticky bit is set on all world-writable directories

Unknown

Description:

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

Rationale:

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

Remediation:

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

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

Assessment:

Ensure sticky bit is set on all world-writable directories -- More

Back to Summary

1.1.21 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 system even if they lacked permissions to mount it themselves.

Remediation:

Run the following command to disable `autofs`:

```
# systemctl disable autofs
```

Impact:

The use 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:

Ensure standard service 'autofs' is disabled -- More

Back to Summary

1.2 Configure Software Updates

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

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

1.3 Filesystem Integrity Checking

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

1.3.1 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:

Run the following command to install AIDE:

```
# apt-get install aide
```

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

Initialize AIDE:

```
# aide --init
```

Assessment:

Ensure package name equals 'aide' is installed -- Less

CIS-CAT expected to collect at least 1 matching dpkg Package, and found 0 items.

Package Name: aide — does not exist

Back to Summary

1.3.2 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:

Run the following command:

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

Add the following line to the crontab:

```
0 5 * * * /usr/bin/aide --check
```

Assessment:

Any of the following tests or sub-groups may pass:

Ensure at least one file(s) named .* in /etc/cron.monthly exists and matches pattern ^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/cron.monthly/0anacron	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	
File:	/etc/cron.monthly/.placeholder	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	

Any of the following tests or sub-groups may pass:

Ensure at least one file(s) named .* in /etc/cron.weekly exists and matches pattern ^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/cron.weekly/0anacron	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	
File:	/etc/cron.weekly/update-notifier-common	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	
File:	/etc/cron.weekly/.placeholder	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	

Any of the following tests or sub-groups may pass:

Ensure at least one file(s) named .* in /etc/cron.daily exists and matches pattern ^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/cron.daily/upstart	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	
File:	/etc/cron.daily/0anacron	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	
File:	/etc/cron.daily/sysstat	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	

Any of the following tests or sub-groups may pass:

Ensure at least one file(s) named .* in /etc/cron.hourly exists and matches pattern ^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/cron.hourly/.placeholder	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	

Any of the following tests or sub-groups may pass:

Ensure at least one file(s) named .* in /etc/cron.d exists and matches pattern ^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/cron.d/sysstat	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	
File:	/etc/cron.d/anacron	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	
File:	/etc/cron.d/.placeholder	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	

Any of the following tests or sub-groups may pass:

Ensure at least one file named /var/spool/cron/crontabs/root exists and matches pattern ^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/var/spool/cron/crontabs/root	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	

Ensure at least one file named /etc/crontab exists and matches pattern ^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/crontab	does not exist
Pattern:	^\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+\S+\s+/usr/bin/aide --check	
Match Text:	No match found	

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 permissions on bootloader config are configured

Fail

Description:

The grub configuration file contains information on boot settings and passwords for unlocking boot options. The grub configuration is usually `grub.cfg` stored in `/boot/grub`.

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 og-rwx /boot/grub/grub.cfg
```

Assessment:

Ensure at least one file named /boot/grub/grub.cfg exists and is owned by 0:0 and does not have permissions ---rwxrwx -- Less

File: /boot/grub/grub.cfg

CIS-CAT Expected...	CIS-CAT Collected...
the file's *Group Execute* to be set to **false**	false
the file's *Other Read* to be set to **false**	true
the file's *Group ID* to be set to **0**	0
the file's *User ID* to be set to **0**	0
the file's *Other Execute* to be set to **false**	false
the file's *Other Write* to be set to **false**	false
the file's *Group Read* to be set to **false**	true
the file's *Group Write* to be set to **false**	false

Back to Summary

1.4.2 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 SELinux at boot time).

Remediation:

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

```
# grub-mkpasswd-pbkdf2
Enter password: <password>
Reenter password: <password>
Your PBKDF2 is <encrypted-password>
```

Add the following into `/etc/grub.d/00_header` or a custom `/etc/grub.d` configuration file:

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

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

```
# update-grub
```

Assessment:

Any of the following tests or sub-groups may pass:

Ensure at least one file named /boot/grub/grub.cfg exists and matches pattern ^\s*set\s+superusers\s*=\s*"[^"]*"\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/boot/grub/grub.cfg	does not exist
Pattern:	^\s*set\s+superusers\s*=\s*"[^"]*"\s*(\s+#.*)?$	
Match Text:	No match found	

Ensure at least one file named /boot/grub/grub.cfg exists and matches pattern ^\s*password_pbkdf2\s+\S+\s+\S+\s+\S+\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/boot/grub/grub.cfg	does not exist
Pattern:	^\s*password_pbkdf2\s+\S+\s+\S+\s+\S+\s*(\s+#.*)?$	
Match Text:	No match found	

Back to Summary

1.5 Additional Process Hardening

1.5.1 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 the `/etc/security/limits.conf` file or a `/etc/security/limits.d/*` file:

```
* hard core 0
```

Set the following parameter in the `/etc/sysctl.conf` file:

```
fs.suid_dumpable = 0
```

Run the following command to set the active kernel parameter:

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

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'fs.suid_dumpable' kernel parameter equals 0 (int) -- Less

Check:	All Must Pass	
Kernel Parameter:	fs.suid_dumpable	
CIS-CAT Expected...		CIS-CAT Collected...
the *Kernel Parameter Name* to be set to **fs.suid_dumpable**		fs.suid_dumpable
the *Kernel Parameter Value* to be set to **0**		2

Any of the following tests or sub-groups may pass:

Ensure at least one file named /etc/security/limits.conf exists and matches pattern ^\s\s+hard\s+core\s+0\s*(\s+#.*)?$ --** Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/security/limits.conf	does not exist
Pattern:	^\s**\s+hard\s+core\s+0\s*(\s+#.*)?$	
Match Text:	No match found	

Ensure at least one file(s) named .* in /etc/security/limits.d exists and matches pattern ^\s\s+hard\s+core\s+0\s*(\s+#.*)?$ --** Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/security/limits.d/.*	
Pattern:	^\s**\s+hard\s+core\s+0\s*(\s+#.*)?$	does not exist
Match Text:	No match found	

Back to Summary

1.5.2 Ensure XD/NX support is enabled

Informational

Description:

Recent processors in the x86 family support the ability to prevent code execution on a per memory page basis. Generically and on AMD processors, this ability is called No Execute (NX), while on Intel processors it is called Execute Disable (XD). This ability can help prevent exploitation of buffer overflow vulnerabilities and should be

activated whenever possible. Extra steps must be taken to ensure that this protection is enabled, particularly on 32-bit x86 systems. Other processors, such as Itanium and POWER, have included such support since inception and the standard kernel for those platforms supports the feature.

Rationale:

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

Remediation:

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

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

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

Assessment:

Ensure 'dmesg | grep "NX [(]Execute Disable[)] protection: active"' output pattern match '.+' (string) -- Less

Check:	At Least One Must Pass
Command:	dmesg | grep "NX [(]Execute Disable[)] protection: active"
Line Selection:	.+

CIS-CAT Expected (At least one of)... CIS-CAT Collected...

the *Std. Output* matches the regular expression **.+**

Back to Summary

1.5.3 Ensure address space layout randomization (ASLR) is enabled

Pass

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 the `/etc/sysctl.conf` file:

```
kernel.randomize_va_space = 2
```

Run the following command to set the active kernel parameter:

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

Assessment:

Ensure 'kernel.randomize_va_space' kernel parameter equals 2 (int) -- More

Back to Summary

1.5.4 Ensure prelink is disabled

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
```

Run the following command to uninstall `prelink`:

```
# apt-get remove prelink
```

Assessment:

Ensure package name equals 'prelink' is not installed -- More

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.

1.6.1 Configure SELinux

SELinux provides a Mandatory Access Control (MAC) system that greatly augments the default Discretionary Access Control (DAC) model. Under SELinux, every process and every object (files, sockets, pipes) on the system is assigned a security context, a label that includes detailed type information about the object. The kernel allows processes to access objects only if that access is explicitly allowed by the policy in effect. The policy defines transitions, so that a user can be allowed to run software, but the software can run under a different context than the user's default. 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 SELinux MAC rules. The action will not be allowed if either one of these models does not permit the action. In this way, SELinux rules can only make a system's permissions more restrictive and secure. SELinux requires a complex policy to allow all the actions required of a system under normal operation. Three such policies have been available for use with Ubuntu and are included with the system: `ubuntu`, `default`, `strict`, and `mls`. These are described as follows:

- `ubuntu`: targeted rules developed for ubuntu specifically
- `default`: targeted rules developed and maintained by Debian. Consists mostly of Type Enforcement (TE) rules, and a small number of Role-Based Access Control (RBAC) rules. Targeted restricts the actions of many types of programs, but leaves interactive users largely unaffected.
- `strict`: also uses TE and RBAC rules, but on more programs and more aggressively.
- `mls`: implements Multi-Level Security (MLS), which introduces even more kinds of labels (sensitivity and category) and rules that govern access based on these.

This section provides guidance for the configuration of the `targeted` policy.

Note: This section only applies if SELinux is in use on the system. Recommendations for AppArmor are also included, and additional Mandatory Access Control systems exist beyond these two. AppArmor is the standard MAC system for Ubuntu systems.

References:

1. NSA SELinux resources:
    1. http://www.nsa.gov/research/selinux
    2. http://www.nsa.gov/research/selinux/list.shtml
2. Fedora SELinux resources:
    1. FAQ: http://docs.fedoraproject.org/selinux-faq
    2. User Guide: http://docs.fedoraproject.org/selinux-user-guide
    3. Managing Services Guide: http://docs.fedoraproject.org/selinux-managing-confined-services-guide

3. SELinux Project web page and wiki:
    1. http://www.selinuxproject.org
4. Chapters 43-45 of Red Hat Enterprise Linux 5: Deployment Guide (Frank Mayer, Karl MacMillan and David Caplan),
5. SELinux by Example: Using Security Enhanced Linux (Prentice Hall, August 6, 2006)

1.6.2 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.

Note: This section only applies if AppArmor is in use on the system. Recommendations for SELinux are also included, and additional Mandatory Access Control systems exist beyond these two.

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/

1.7 Warning Banners

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

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

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

1.7.1 Command Line Warning Banners

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

1.7.1.1 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`, or `\v`.

Assessment:

Ensure at least one file named /etc/motd exists and does not match pattern (\\v|\\r|\\m|\\s) -- More

Back to Summary

1.7.1.2 Ensure local login warning banner is configured properly

Informational

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

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`, or `\v`:

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

Assessment:

Ensure at least one file named /etc/issue exists and does not match pattern (\\v|\\r|\\m|\\s) -- More

Back to Summary

1.7.1.3 Ensure remote login warning banner is configured properly

Informational

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`, or `\v`:

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

Assessment:

Ensure at least one file named /etc/issue.net exists and does not match pattern (\\v|\\r|\\m|\\s) -- More

Back to Summary

1.7.1.4 Ensure permissions on /etc/motd are configured

Informational

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 /etc/motd
# chmod 644 /etc/motd
```

Assessment:

Ensure at least one file named /etc/motd exists and is owned by 0:0 and has permissions rw-r--r-- and does not have permissions --x-wx-wx SUID SGID sticky -- Less

CIS-CAT expected at least 1 matching file item to be collected, and found 0 items.
File: /etc/motd does not exist

Back to Summary

1.7.1.5 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 /etc/issue
# chmod 644 /etc/issue
```

Assessment:

Ensure at least one file named /etc/issue exists and is owned by 0:0 and has permissions rw-r--r-- and does not have permissions --x-wx-wx SUID SGID sticky -- More

Back to Summary

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

Informational

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 /etc/issue.net
# chmod 644 /etc/issue.net
```

Assessment:

Ensure at least one file named /etc/issue.net exists and is owned by 0:0 and has permissions rw-r--r-- and does not have permissions --x-wx-wx SUID SGID sticky -- More

Back to Summary

1.7.2 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:

Create the `/etc/dconf/profile/gdm` file with the following contents:

```
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

Create or edit the `banner-message-enable` and `banner-message-text` options in `/etc/dconf/db/gdm.d/01-banner-message`:

```
[org/gnome/login-screen]
banner-message-enable=true
banner-message-text='Authorized uses only. All activity may be monitored and reported.'
```

Run the following command to update the system databases:

```
# dconf update
```

Assessment:

Any of the following tests or sub-groups may pass:

Ensure package name equals 'gdm' is not installed -- More

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/dconf/db/gdm.d/01-banner-message exists and matches pattern ^banner-message-text='.+'$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/dconf/db/gdm.d/01-banner-message	does not exist
Pattern:	^banner-message-text='.+'$	
Match Text:	No match found	

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/dconf/db/gdm.d/01-banner-message exists and matches pattern ^banner-message-enable=true$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/dconf/db/gdm.d/01-banner-message	does not exist
Pattern:	^banner-message-enable=true$	
Match Text:	No match found	

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/dconf/profile/gdm exists and matches pattern ^file-db:/usr/share/gdm/greeter-dconf-defaults$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/dconf/profile/gdm	does not exist
Pattern:	^file-db:/usr/share/gdm/greeter-dconf-defaults$	
Match Text:	No match found	

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/dconf/profile/gdm exists and matches pattern ^user-db:user$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/dconf/profile/gdm	does not exist
Pattern:	^user-db:user$	
Match Text:	No match found	

Ensure at least one file named /etc/dconf/profile/gdm exists and matches pattern ^system-db:gdm$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/dconf/profile/gdm	does not exist
Pattern:	^system-db:gdm$	
Match Text:	No match found	

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.

2.1 inetd Services

inetd is a super-server daemon that provides internet services and passes connections to configured services. While not commonly used inetd and any unneeded inetd based services should be disabled if possible.

2.1.1 Ensure chargen services are not enabled

Pass

Description:

`chargen` is a network service that responds with 0 to 512 ASCII characters for each connection it receives. This service is intended for debugging and testing purposes. It is recommended that this service be disabled.

Rationale:

Disabling this service will reduce the remote attack surface of the system.

Remediation:

Comment out or remove any lines starting with `chargen` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `chargen` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Assessment:

All of the following tests or sub-groups must pass:
Ensure inted service 'chargen' is disabled -- More
Ensure inted service 'chargen' is disabled -- More
Ensure inted service 'chargen' is disabled -- More

Back to Summary

2.1.2 Ensure daytime services are not enabled

Pass

Description:

`daytime` is a network service that responds with the server's current date and time. This service is intended for debugging and testing purposes. It is recommended that this service be disabled.

Rationale:

Disabling this service will reduce the remote attack surface of the system.

Remediation:

Comment out or remove any lines starting with `daytime` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `daytime` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Assessment:

All of the following tests or sub-groups must pass:
Ensure inted service 'daytime' is disabled -- More
Ensure inted service 'daytime' is disabled -- More
Ensure inted service 'daytime' is disabled -- More

Back to Summary

2.1.3 Ensure discard services are not enabled

Pass

Description:

`discard` is a network service that simply discards all data it receives. This service is intended for debugging and testing purposes. It is recommended that this service be disabled.

Rationale:

Disabling this service will reduce the remote attack surface of the system.

Remediation:

Comment out or remove any lines starting with `discard` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `discard` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Assessment:

All of the following tests or sub-groups must pass:
Ensure inted service 'discard' is disabled -- More
Ensure inted service 'discard' is disabled -- More
Ensure inted service 'discard' is disabled -- More

Back to Summary

2.1.4 Ensure echo services are not enabled

Pass

Description:

`echo` is a network service that responds to clients with the data sent to it by the client. This service is intended for debugging and testing purposes. It is recommended that this service be disabled.

Rationale:

Disabling this service will reduce the remote attack surface of the system.

Remediation:

Comment out or remove any lines starting with `echo` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `echo` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Assessment:

All of the following tests or sub-groups must pass:
Ensure inted service 'echo' is disabled -- More
Ensure inted service 'echo' is disabled -- More
Ensure inted service 'echo' is disabled -- More

Back to Summary

2.1.5 Ensure time services are not enabled

Pass

Description:

`time` is a network service that responds with the server's current date and time as a 32 bit integer. This service is intended for debugging and testing purposes. It is recommended that this service be disabled.

Rationale:

Disabling this service will reduce the remote attack surface of the system.

Remediation:

Comment out or remove any lines starting with `time` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `time` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Assessment:

All of the following tests or sub-groups must pass:

Ensure inted service 'time' is disabled -- More
Ensure inted service 'time' is disabled -- More
Ensure inted service 'time' is disabled -- More

Back to Summary

2.1.6 Ensure rsh server is not enabled

Pass

Description:

The Berkeley `rsh-server` (`rsh`, `rlogin`, `rexec`) package contains legacy services that exchange credentials in clear-text.

Rationale:

These legacy services contain numerous security exposures and have been replaced with the more secure SSH package.

Remediation:

Comment out or remove any lines starting with `shell`, `login`, or `exec` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `rsh`, `rlogin`, and `rexec` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Assessment:

All of the following tests or sub-groups must pass:
Ensure inted service 'resec' is disabled -- More
Ensure inted service 'resec' is disabled -- More
Ensure inted service 'resec' is disabled -- More
All of the following tests or sub-groups must pass:
Ensure inted service 'rlogin' is disabled -- More
Ensure inted service 'rlogin' is disabled -- More
Ensure inted service 'rlogin' is disabled -- More
All of the following tests or sub-groups must pass:
Ensure inted service 'rsh' is disabled -- More
Ensure inted service 'rsh' is disabled -- More
Ensure inted service 'rsh' is disabled -- More
All of the following tests or sub-groups must pass:
Ensure inted service 'exec' is disabled -- More
Ensure inted service 'exec' is disabled -- More
Ensure inted service 'exec' is disabled -- More
All of the following tests or sub-groups must pass:
Ensure inted service 'login' is disabled -- More
Ensure inted service 'login' is disabled -- More
Ensure inted service 'login' is disabled -- More
Ensure inted service 'shell' is disabled -- More
Ensure inted service 'shell' is disabled -- More
Ensure inted service 'shell' is disabled -- More

Back to Summary

2.1.7 Ensure talk server is not enabled

Pass

Description:

The talk software makes it possible for users to send and receive messages across systems through a terminal session. The talk client (allows initiate of talk sessions) is installed by default.

Rationale:

The software presents a security risk as it uses unencrypted protocols for communication.

Remediation:

Comment out or remove any lines starting with `talk` or `ntalk` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `talk` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Assessment:

All of the following tests or sub-groups must pass:
Ensure inted service 'talk' is disabled -- More
Ensure inted service 'talk' is disabled -- More
Ensure inted service 'talk' is disabled -- More
Ensure inted service 'ntalk' is disabled -- More
Ensure inted service 'ntalk' is disabled -- More
Ensure inted service 'ntalk' is disabled -- More

Back to Summary

2.1.8 Ensure telnet server is not enabled

Pass

Description:

The `telnet-server` package contains the `telnet` daemon, which accepts connections from users from other systems via the `telnet` protocol.

Rationale:

The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow a user with access to sniff network traffic the ability to steal credentials. The `ssh` package provides an encrypted session and stronger security.

Remediation:

Comment out or remove any lines starting with `telnet` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `telnet` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Assessment:

All of the following tests or sub-groups must pass:
Ensure inted service 'telnet' is disabled -- More
Ensure inted service 'telnet' is disabled -- More
Ensure inted service 'telnet' is disabled -- More

Back to Summary

2.1.9 Ensure tftp server is not enabled

Pass

Description:

Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol, typically used to automatically transfer configuration or boot machines from a boot server. The packages `tftp` and `atftp` are both used to define and support a TFTP server.

Rationale:

TFTP does not support authentication nor does it ensure the confidentiality or integrity of data. It is recommended that TFTP be removed, unless there is a specific need for TFTP. In that case, extreme caution must be used when configuring the services.

Remediation:

Comment out or remove any lines starting with `tftp` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `tftp` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Assessment:

All of the following tests or sub-groups must pass:

Ensure inted service 'tftp' is disabled -- More
Ensure inted service 'tftp' is disabled -- More
Ensure inted service 'tftp' is disabled -- More

Back to Summary

2.1.10 Ensure xinetd is not enabled

Fail

Description:

The eXtended InterNET Daemon (`xinetd`) is an open source super daemon that replaced the original `inetd` daemon. The `xinetd` daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests.

Rationale:

If there are no `xinetd` services required, it is recommended that the daemon be disabled.

Remediation:

Run the following command to disable `xinetd`:

```
# systemctl disable xinetd
```

Assessment:

Ensure standard service 'xinetd' is disabled -- Less

Check:	All Must Pass	
Command:	systemctl is-enabled xinetd.service	
Line Selection:	enabled	
CIS-CAT Expected (At least one of)...		CIS-CAT Collected...
the *Std. Output* does not match the regular expression **.+**		enabled

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 disabled or deleted from the system to reduce the potential attack surface.

2.2.1 Time Synchronization

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

2.2.1.1 Ensure time synchronization is in use

Informational

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.

Rationale:

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

Remediation:

On physical systems or virtual systems where host based time synchronization is not available install NTP or chrony using one of the following commands:

```
# apt-get install ntp
# apt-get install chrony
```

On virtual systems where host based time synchronization is available consult your virtualization software documentation and setup host based synchronization.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure package name equals 'chrony' is installed -- Less

CIS-CAT expected to collect at least 1 matching dpkg Package, and found 0 items.
Package Name: chrony does not exist

Ensure package name equals 'ntp' is installed -- Less

CIS-CAT expected to collect at least 1 matching dpkg Package, and found 0 items.
Package Name: ntp does not exist

Back to Summary

2.2.1.2 Ensure ntp is configured

Pass

Description:

`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.

This recommendation only applies if ntp is in use on the system.

Rationale:

If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

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
```

Add or edit server lines to `/etc/ntp.conf` as appropriate:

```
server <remote-server>
```

Configure `ntp` to run as the `ntp` user by adding or editing the following file:

`/etc/init.d/ntp`:

```
RUNASUSER=ntp
```

Assessment:

Any of the following tests or sub-groups may pass:

Ensure package name equals 'ntp' is not installed -- More

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/init.d/ntp exists and matches pattern ^\s*RUNASUSER\s*=\s*ntp\s*(?:#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/init.d/ntp	does not exist
Pattern:	^\s*RUNASUSER\s*=\s*ntp\s*(?:#.*)?$	
Match Text:	No match found	

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/ntp.conf exists and matches pattern ^\s*server\s+\S+ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/ntp.conf	does not exist
Pattern:	^\s*server\s+\S+	
Match Text:	No match found	

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/ntp.conf exists and matches pattern ^\s*restrict\s+(-4\s+)?default(?=[^#]*\s+kod)(?=[^#]*\s+nomodify)(?=[^#]*\s+notrap)(?=[^#]*\s+nopeer)(?=[^#]*\s+noquery)(\s+kod|\s+nomodify|\s+notrap|\s+nopeer|\s+noquery)*\s*(?:#.*)? -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/ntp.conf	does not exist
Pattern:	^\s*restrict\s+(-4\s+)?default(?=[^#]*\s+kod)(?=[^#]*\s+nomodify)(?=[^#]*\s+notrap)(?=[^#]*\s+nopeer)(?=[^#]*\s+noquery)(\s+kod|\s+nomodify|\s+notrap|\s+nopeer|\s+noquery)*\s*(?:#.*)?$	
Match Text:	No match found	

Ensure at least one file named /etc/ntp.conf exists and matches pattern ^\s*restrict\s+-6\s+default(?=[^#]*\s+kod)(?=[^#]*\s+nomodify)(?=[^#]*\s+notrap)(?=[^#]*\s+nopeer)(?=[^#]*\s+noquery)(\s+kod|\s+nomodify|\s+notrap|\s+nopeer|\s+noquery)*\s*(?:#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/ntp.conf	does not exist
Pattern:	^\s*restrict\s+-6\s+default(?=[^#]*\s+kod)(?=[^#]*\s+nomodify)(?=[^#]*\s+notrap)(?=[^#]*\s+nopeer)(?=[^#]*\s+noquery)(\s+kod|\s+nomodify|\s+notrap|\s+nopeer|\s+noquery)*\s*(?:#.*)?$	
Match Text:	No match found	

Back to Summary

2.2.1.3 Ensure chrony is configured

Pass

Description:

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

Rationale:

If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

This recommendation only applies if chrony is in use on the system.

Remediation:

Add or edit server lines to `/etc/chrony/chrony.conf` as appropriate:

```
server <remote-server>
```

Configure `chrony` to run as the `chrony` user by configuring the appropriate startup script for your distribution. Startup scripts are typically stored in `/etc/init.d` or `/etc/systemd`.

Assessment:

Any of the following tests or sub-groups may pass:
Ensure package name equals 'chrony' is not installed -- More
All of the following tests or sub-groups must pass:
Linux Custom Object "chronyd is running as chrony user" -- More
Ensure at least one file named /etc/chrony/chrony.conf exists and matches pattern ^\s*server\s+\S+ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/chrony/chrony.conf	does not exist
Pattern:	^\s*server\s+\S+	
Match Text:	No match found	

Back to Summary

2.2.2 Ensure X Window System is not installed

Fail

Description:

The X Window System provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Windows system is typically used on workstations where users login, but not on servers where users typically do not login.

Rationale:

Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.

Remediation:

Run the following command to remove the X Windows System packages:

```
apt-get remove xserver-xorg*
```

Assessment:

Ensure package name pattern match '^xserver-xorg.*' is not installed -- Less

CIS-CAT did not expect to collect any matching dpkg Packages, and found 17 items.

Package Name: xserver-xorg-core-hwe-16.04	exists
Package Name: xserver-xorg-hwe-16.04	exists
Package Name: xserver-xorg-input-all-hwe-16.04	exists
Package Name: xserver-xorg-input-evdev-hwe-16.04	exists
Package Name: xserver-xorg-input-synaptics-hwe-16.04	exists
Package Name: xserver-xorg-input-wacom-hwe-16.04	exists
Package Name: xserver-xorg-legacy-hwe-16.04	exists
Package Name: xserver-xorg-video-all-hwe-16.04	exists
Package Name: xserver-xorg-video-amdgpu-hwe-16.04	exists
Package Name: xserver-xorg-video-ati-hwe-16.04	exists

Back to Summary

2.2.3 Ensure Avahi Server is not enabled

Fail

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 disable the service to reduce the potential attach surface.

Remediation:

Run the following command to disable `avahi-daemon`:

```
# systemctl disable avahi-daemon
```

Assessment:

Ensure standard service 'avahi-daemon' is disabled -- Less

Check:	All Must Pass
Command:	systemctl is-enabled avahi-daemon.service
Line Selection:	enabled

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* does not match the regular expression **.+**	enabled

Back to Summary

2.2.4 Ensure CUPS is not enabled

Fail

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 disabled to reduce the potential attack surface.

Remediation:

Run the following command to disable `cups`:

```
# systemctl disable cups
```

Impact:

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

Assessment:

Ensure standard service 'cups' is disabled -- Less

Check:	All Must Pass
Command:	systemctl is-enabled cups.service
Line Selection:	enabled

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* does not match the regular expression **.+**	enabled

Back to Summary

2.2.5 Ensure DHCP Server is not enabled

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 service be deleted to reduce the potential attack surface.

Remediation:

Run the following commands to disable dhcpd:

```
# systemctl disable isc-dhcp-server
# systemctl disable isc-dhcp-server6
```

Assessment:

All of the following tests or sub-groups must pass:
Ensure standard service 'isc-dhcp-server' is disabled -- More
Ensure standard service 'isc-dhcp-server6' is disabled -- More

Back to Summary

2.2.6 Ensure LDAP server is not enabled

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 disabled to reduce the potential attack surface.

Remediation:

Run the following command to disable `slapd`:

```
# systemctl disable slapd
```

Assessment:

Ensure standard service 'slapd' is disabled -- More

Back to Summary

2.2.7 Ensure NFS and RPC are not enabled

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 or act as an NFS client, it is recommended that these services be disabled to reduce remote attack surface.

Remediation:

Run the following commands to disable `nfs` and `rpcbind`:

```
# systemctl disable nfs-kernel-server
# systemctl disable rpcbind
```

Assessment:

All of the following tests or sub-groups must pass:
Ensure standard service 'nfs-kernel-server' is disabled -- More
Ensure standard service 'rpcbind' is disabled -- More

Back to Summary

2.2.8 Ensure DNS Server is not enabled

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 command to disable `named`:

```
# systemctl disable bind9
```

Assessment:

Ensure standard service 'bind9' is disabled -- More

Back to Summary

2.2.9 Ensure FTP Server is not enabled

Fail

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 disable `vsftpd`:

```
# systemctl disable vsftpd
```

Assessment:

Ensure standard service 'vsftpd' is disabled -- Less

Check:	All Must Pass
Command:	systemctl is-enabled vsftpd.service
Line Selection:	enabled

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* does not match the regular expression **.+**	enabled

Back to Summary

2.2.10 Ensure HTTP server is not enabled

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 disable `apache2`:

```
# systemctl disable apache2
```

Assessment:

Ensure standard service 'apache2' is disabled -- Less

Check:	All Must Pass
Command:	systemctl is-enabled apache2.service
Line Selection:	enabled

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* does not match the regular expression **.+**	enabled

Back to Summary

2.2.11 Ensure IMAP and POP3 server is not enabled

Pass

Description:

`dovecot` is an open source IMAP and POP3 server for Linux based systems.

Rationale:

Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the service be deleted to reduce the potential attack surface.

Remediation:

Run the following command to disable `dovecot`:

```
# systemctl disable dovecot
```

Assessment:

Ensure standard service 'dovecot' is disabled -- More

Back to Summary

2.2.12 Ensure Samba is not enabled

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 Small 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 can be deleted to reduce the potential attack surface.

Remediation:

Run the following command to disable `smbd`:

```
# systemctl disable smbd
```

Assessment:

Ensure standard service 'smbd' is disabled -- More

Back to Summary

2.2.13 Ensure HTTP Proxy Server is not enabled

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 disable `squid`:

```
# systemctl disable squid
```

Assessment:

Ensure standard service 'squid' is disabled -- More

Back to Summary

2.2.14 Ensure SNMP Server is not enabled

Pass

Description:

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 communicates using SNMP v1, which transmits data in the clear and does not require authentication to execute commands. Unless absolutely necessary, it is recommended that the SNMP service not be used.

Remediation:

Run the following command to disable `snmpd`:

```
# systemctl disable snmpd
```

Assessment:

Ensure standard service 'snmpd' is disabled -- More

Back to Summary

2.2.15 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.

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 = localhost
```

Restart postfix:

```
# service postfix restart
```

Assessment:

Linux Custom Object "No Servers Listening On Port 25" -- More

Back to Summary

2.2.16 Ensure rsync service is not enabled

Pass

Description:

The `rsyncd` service can be used to synchronize files between systems over network links.

Rationale:

The `rsyncd` service presents a security risk as it uses unencrypted protocols for communication.

Remediation:

Run the following command to disable `rsync`:

```
# systemctl disable rsync
```

Assessment:

Ensure standard service 'rsync' is disabled -- More

Back to Summary

2.2.17 Ensure NIS Server is not enabled

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 been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be disabled and other, more secure services be used

Remediation:

Run the following command to disable `nis`:

```
# systemctl disable nis
```

Assessment:

Ensure standard service 'nis' is disabled -- 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 (`ypbind`) was used to bind a machine to an NIS server and receive the distributed configuration files.

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

Remediation:

Run the following command to uninstall nis :

```
apt-get remove 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:

Ensure package name equals 'nis' is not installed -- More

Back to Summary

2.3.2 Ensure rsh client is not installed

Pass

Description:

The `rsh` package contains the client commands for the rsh services.

Rationale:

These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the `rsh` package removes the clients for `rsh`, `rcp` and `rlogin`.

Remediation:

Run the following command to uninstall `rsh`:

```
apt-get remove rsh-client rsh-redone-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:

All of the following tests or sub-groups must pass:
Ensure package name equals 'rsh-redone-client' is not installed -- More
Ensure package name equals 'rsh-client' is not installed -- 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:

Run the following command to uninstall `talk`:

```
apt-get remove 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:

Ensure package name equals 'talk' is not installed -- 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:

Run the following command to uninstall `telnet`:

```
# apt-get remove 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:

Ensure package name equals 'telnet' is not installed -- Less

CIS-CAT did not expect to collect any matching dpkg Packages, and found 1 item.
Package Name: telnet exists

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` using the appropriate package manager or manual installation:

```
# apt-get remove ldap-utils
```

Impact:

Removing the LDAP client will prevent or inhibit using LDAP for authentication in your environment.

Assessment:

Ensure package name equals 'ldap-utils' is not installed -- 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.

3.1 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.

3.1.1 Ensure IP forwarding is disabled

Pass

Description:

The `net.ipv4.ip_forward` flag is used to tell the system whether it can forward packets or not.

Rationale:

Setting the flag 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 the `/etc/sysctl.conf` file:

```
net.ipv4.ip_forward = 0
```

Run the following commands to set the active kernel parameters:

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

Assessment:

Ensure 'net.ipv4.ip_forward' kernel parameter equals 0 (int) -- More

Back to Summary

3.1.2 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 the `/etc/sysctl.conf` file:

```
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.send_redirects=0
# sysctl -w net.ipv4.conf.default.send_redirects=0
# sysctl -w net.ipv4.route.flush=1
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'net.ipv4.conf.all.send_redirects' kernel parameter equals 0 (int) -- Less

Check:	All Must Pass	
Kernel Parameter:	net.ipv4.conf.all.send_redirects	
CIS-CAT Expected...		CIS-CAT Collected...
the *Kernel Parameter Name* to be set to **net.ipv4.conf.all.send_redirects**		net.ipv4.conf.all.send_redirects
the *Kernel Parameter Value* to be set to **0**		1

Ensure 'net.ipv4.conf.default.send_redirects' kernel parameter equals 0 (int) -- Less

Check:	All Must Pass	
Kernel Parameter:	net.ipv4.conf.default.send_redirects	
CIS-CAT Expected...		CIS-CAT Collected...
the *Kernel Parameter Name* to be set to **net.ipv4.conf.default.send_redirects**		net.ipv4.conf.default.send_redirects
the *Kernel Parameter Value* to be set to **0**		1

Back to Summary

3.2 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.

3.2.1 Ensure source routed packets are not accepted

Pass

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` and `net.ipv4.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 the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.accept_source_route=0
# sysctl -w net.ipv4.conf.default.accept_source_route=0
# sysctl -w net.ipv4.route.flush=1
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'net.ipv4.conf.all.accept_source_route' kernel parameter equals 0 (int) -- More

Ensure 'net.ipv4.conf.default.accept_source_route' kernel parameter equals 0 (int) -- More

Back to Summary

3.2.2 Ensure ICMP redirects are not accepted

Pass

Description:

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting `net.ipv4.conf.all.accept_redirects` to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Rationale:

Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.accept_redirects=0
# sysctl -w net.ipv4.conf.default.accept_redirects=0
# sysctl -w net.ipv4.route.flush=1
```

Assessment:

All of the following tests or sub-groups must pass:
Ensure 'net.ipv4.conf.all.accept_redirects' kernel parameter equals 0 (int) -- More
Ensure 'net.ipv4.conf.all.accept_redirects' kernel parameter equals 0 (int) -- More

Back to Summary

3.2.3 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` to 0 protects the system from routing table updates by possibly compromised known gateways.

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

```
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.secure_redirects=0
# sysctl -w net.ipv4.conf.default.secure_redirects=0
# sysctl -w net.ipv4.route.flush=1
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'net.ipv4.conf.all.secure_redirects' kernel parameter equals 0 (int) -- Less

Check:	All Must Pass	
Kernel Parameter:	net.ipv4.conf.all.secure_redirects	
CIS-CAT Expected...		CIS-CAT Collected...
the *Kernel Parameter Name* to be set to **net.ipv4.conf.all.secure_redirects**		net.ipv4.conf.all.secure_redirects
the *Kernel Parameter Value* to be set to **0**		1

Ensure 'net.ipv4.conf.default.secure_redirects' kernel parameter equals 0 (int) -- Less

Check:	All Must Pass	
Kernel Parameter:	net.ipv4.conf.default.secure_redirects	
CIS-CAT Expected...		CIS-CAT Collected...
the *Kernel Parameter Name* to be set to **net.ipv4.conf.default.secure_redirects**		net.ipv4.conf.default.secure_redirects
the *Kernel Parameter Value* to be set to **0**		1

Back to Summary

3.2.4 Ensure suspicious packets are logged

Fail

Description:

When enabled, this feature logs packets with un-routable source addresses to the kernel log.

Rationale:

Enabling this feature and logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

```
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.log_martians=1
# sysctl -w net.ipv4.conf.default.log_martians=1
# sysctl -w net.ipv4.route.flush=1
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'net.ipv4.conf.all.log_martians' kernel parameter equals 1 (int) -- Less

Check:	All Must Pass	
Kernel Parameter:	net.ipv4.conf.all.log_martians	
CIS-CAT Expected...		CIS-CAT Collected...
the *Kernel Parameter Name* to be set to **net.ipv4.conf.all.log_martians**		net.ipv4.conf.all.log_martians
the *Kernel Parameter Value* to be set to **1**		0

Ensure 'net.ipv4.conf.default.log_martians' kernel parameter equals 1 (int) -- Less

Check:	All Must Pass	
Kernel Parameter:	net.ipv4.conf.default.log_martians	
CIS-CAT Expected...		CIS-CAT Collected...
the *Kernel Parameter Name* to be set to **net.ipv4.conf.default.log_martians**		net.ipv4.conf.default.log_martians
the *Kernel Parameter Value* to be set to **1**		0

Back to Summary

3.2.5 Ensure broadcast ICMP requests are ignored

Pass

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 the `/etc/sysctl.conf` file:

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
# sysctl -w net.ipv4.route.flush=1
```

Assessment:

Ensure 'net.ipv4.icmp_echo_ignore_broadcasts' kernel parameter equals 1 (int) -- More

Back to Summary

3.2.6 Ensure bogus ICMP responses are ignored

Pass

Description:

Setting `icmp_ignore_bogus_error_responses` to 1 prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages.

Rationale:

Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

Remediation:

Set the following parameter in the `/etc/sysctl.conf` file:

```
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
# sysctl -w net.ipv4.route.flush=1
```

Assessment:

Ensure 'net.ipv4.icmp_ignore_bogus_error_responses' kernel parameter equals 1 (int) -- More

Back to Summary

3.2.7 Ensure Reverse Path Filtering is enabled

Pass

Description:

Setting `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` to 1 forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the packet is dropped (and logged if `log_martians` is set).

Rationale:

Setting these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

```
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.rp_filter=1
# sysctl -w net.ipv4.conf.default.rp_filter=1
# sysctl -w net.ipv4.route.flush=1
```

Assessment:

All of the following tests or sub-groups must pass:
Ensure 'net.ipv4.conf.default.rp_filter' kernel parameter equals 1 (int) -- More
Ensure 'net.ipv4.conf.all.rp_filter' kernel parameter equals 1 (int) -- More

Back to Summary

3.2.8 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. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Remediation:

Set the following parameter in the `/etc/sysctl.conf` file:

```
net.ipv4.tcp_syncookies = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.tcp_syncookies=1
# sysctl -w net.ipv4.route.flush=1
```

Assessment:

Ensure 'net.ipv4.tcp_syncookies' kernel parameter equals 1 (int) -- Less

Check:	All Must Pass	
Kernel Parameter:	net.ipv4.tcp_syncookies	
CIS-CAT Expected...		CIS-CAT Collected...
the *Kernel Parameter Name* to be set to **net.ipv4.tcp_syncookies**		net.ipv4.tcp_syncookies
the *Kernel Parameter Value* to be set to **1**		0

Back to Summary

3.3 IPv6

IPv6 is a networking protocol that supersedes IPv4. It has more routable addresses and has built in security. If IPv6 is to be used, follow this section of the benchmark to configure IPv6, otherwise disable IPv6.

3.3.1 Ensure IPv6 router advertisements are not accepted

Informational

Description:

This setting disables the system's ability to accept IPv6 router advertisements.

Rationale:

It is recommended that systems 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.

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

```
net.ipv6.conf.all.accept_ra = 0
net.ipv6.conf.default.accept_ra = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv6.conf.all.accept_ra=0
# sysctl -w net.ipv6.conf.default.accept_ra=0
# sysctl -w net.ipv6.route.flush=1
```

Assessment:

Any of the following tests or sub-groups may pass:

Ensure at least one file named /boot/grub/grub.cfg exists and matches pattern ^\s*kernel\S+(\s+\S+)+\s+ipv6\.disable=1^\s*linux\S*(\s+\S+)+\s+ipv6\.disable=1 -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/boot/grub/grub.cfg	does not exist
Pattern:	^\s*kernel\S+(\s+\S+)+\s+ipv6\.disable=1^\s*linux\S*(\s+\S+)+\s+ipv6\.disable=1	
Match Text:	No match found	

All of the following tests or sub-groups must pass:

Ensure 'net.ipv6.conf.default.accept_ra' kernel parameter equals 0 (int) -- Less

Check:	All Must Pass
Kernel Parameter:	net.ipv6.conf.default.accept_ra

CIS-CAT Expected...	CIS-CAT Collected...
the *Kernel Parameter Name* to be set to **net.ipv6.conf.default.accept_ra**	net.ipv6.conf.default.accept_ra
the *Kernel Parameter Value* to be set to **0**	1

Ensure 'net.ipv6.conf.all.accept_ra' kernel parameter equals 0 (int) -- Less

Check:	All Must Pass
Kernel Parameter:	net.ipv6.conf.all.accept_ra

CIS-CAT Expected...	CIS-CAT Collected...
the *Kernel Parameter Name* to be set to **net.ipv6.conf.all.accept_ra**	net.ipv6.conf.all.accept_ra
the *Kernel Parameter Value* to be set to **0**	1

Back to Summary

3.3.2 Ensure IPv6 redirects are not accepted

Informational

Description:

This setting prevents the system from accepting ICMP redirects. ICMP redirects tell the system about alternate routes for sending traffic.

Rationale:

It is recommended that systems not accept ICMP redirects 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.

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

```
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv6.conf.all.accept_redirects=0
# sysctl -w net.ipv6.conf.default.accept_redirects=0
# sysctl -w net.ipv6.route.flush=1
```

Assessment:

Any of the following tests or sub-groups may pass:

Ensure at least one file named /boot/grub/grub.cfg exists and matches pattern ^\s*linux\S*(\s+\S+)+\s+ipv6\.disable=1 -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/boot/grub/grub.cfg	does not exist
Pattern:	^\s*linux\S*(\s+\S+)+\s+ipv6\.disable=1	
Match Text:	No match found	

All of the following tests or sub-groups must pass:

Ensure 'net.ipv6.conf.all.accept_redirects' kernel parameter equals 0 (int) -- More

Ensure 'net.ipv6.conf.default.accept_redirects' kernel parameter equals 0 (int) -- More

Back to Summary

3.3.3 Ensure IPv6 is disabled

Informational

Description:

Although IPv6 has many advantages over IPv4, few organizations have implemented IPv6.

Rationale:

If IPv6 is not to be used, it is recommended that it be disabled to reduce the attack surface of the system.

Remediation:

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

```
GRUB_CMDLINE_LINUX="ipv6.disable=1"
```

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

```
# update-grub
```

Assessment:

Ensure at least one file named /boot/grub/grub.cfg exists and matches pattern ^\s*linux\S*(\s+\S+)+\s+ipv6\.disable=1 -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/boot/grub/grub.cfg	does not exist
Pattern:	^\s*linux\S*(\s+\S+)+\s+ipv6\.disable=1	
Match Text:	No match found	

Back to Summary

3.4 TCP Wrappers

3.4.1 Ensure TCP Wrappers is installed

Pass

Description:

TCP Wrappers provides a simple access list and standardized logging method for services capable of supporting it. In the past, services that were called from `inetd` and `xinetd` supported the use of tcp wrappers. As `inetd` and `xinetd` have been falling in disuse, any service that can support tcp wrappers will have the `libwrap.so` library attached to it.

Rationale:

TCP Wrappers provide a good simple access list mechanism to services that may not have that support built in. It is recommended that all services that can support TCP Wrappers, use it.

Remediation:

Run the following command to install TCP Wrappers:

```
apt-get install tcpd
```

Assessment:

Ensure package name equals 'tcpd' is installed -- More

Back to Summary

3.4.2 Ensure /etc/hosts.allow is configured

Pass

Description:

The `/etc/hosts.allow` file specifies which IP addresses are permitted to connect to the host. It is intended to be used in conjunction with the `/etc/hosts.deny` file.

Rationale:

The `/etc/hosts.allow` file supports access control by IP and helps ensure that only authorized systems can connect to the system.

Remediation:

Run the following command to create `/etc/hosts.allow`:

```
# echo "ALL: <net>/<mask>, <net>/<mask>, ..." >/etc/hosts.allow
```

where each *<net>/<mask>* combination (for example, "192.168.1.0/255.255.255.0") represents one network block in use by your organization that requires access to this system.

Assessment:

Ensure at least one file named /etc/hosts.allow exists and unknown test -- More

Back to Summary

3.4.3 Ensure /etc/hosts.deny is configured

Fail

Description:

The `/etc/hosts.deny` file specifies which IP addresses are **not** permitted to connect to the host. It is intended to be used in conjunction with the `/etc/hosts.allow` file.

Rationale:

The `/etc/hosts.deny` file serves as a failsafe so that any host not specified in `/etc/hosts.allow` is denied access to the system.

Remediation:

Run the following command to create `/etc/hosts.deny`:

```
# echo "ALL: ALL" >> /etc/hosts.deny
```

Assessment:

Ensure at least one file named /etc/hosts.deny exists and matches pattern ^ALL: ALL -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/hosts.deny	does not exist
Pattern:	^ALL: ALL	
Match Text:	No match found	

Back to Summary

3.4.4 Ensure permissions on /etc/hosts.allow are configured

Pass

Description:

The `/etc/hosts.allow` file contains networking information that is used by many applications and therefore must be readable for these applications to operate.

Rationale:

It is critical to ensure that the `/etc/hosts.allow` 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 set permissions on `/etc/hosts.allow`:

```
# chown root:root /etc/hosts.allow
# chmod 644 /etc/hosts.allow
```

Assessment:

Ensure at least one file named /etc/hosts.allow exists and is owned by 0:0 and has permissions rw-r--r-- and does not have permissions --x-wx-wx SUID SGID sticky -- More

Back to Summary

3.4.5 Ensure permissions on /etc/hosts.deny are 644

Pass

Description:

The `/etc/hosts.deny` file contains network information that is used by many system applications and therefore must be readable for these applications to operate.

Rationale:

It is critical to ensure that the `/etc/hosts.deny` 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 set permissions on `/etc/hosts.deny`:

```
# chown root:root /etc/hosts.deny
# chmod 644 /etc/hosts.deny
```

Assessment:

Ensure at least one file named /etc/hosts.deny exists and is owned by 0:0 and has permissions rw-r--r-- and does not have permissions --x-wx-wx SUID SGID sticky -- More

Back to Summary

3.5 Uncommon Network Protocols

The Linux kernel modules support several network protocols that are not commonly used. If these protocols are not needed, it is recommended that they be disabled in the kernel.

Note: This should not be considered a comprehensive list of uncommon network protocols, you may wish to consider additions to those listed here for your environment.

3.5.1 Ensure DCCP is disabled

Informational

Description:

The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery.

Rationale:

If the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install dccp /bin/true
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure kernel module dccp is not loadable -- Less

Check:	At Least One Must Pass
Command:	modprobe -n -v dccp
Line Selection:	.+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/net/dccp/dccp.ko

Ensure kernel module dccp is not loaded -- More

Back to Summary

3.5.2 Ensure SCTP is disabled

Informational

Description:

The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP.

Rationale:

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install sctp /bin/true
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure kernel module sctp is not loadable -- Less

Check:	At Least One Must Pass
Command:	modprobe -n -v sctp
Line Selection:	.+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/net/sctp/sctp.ko

Ensure kernel module sctp is not loaded -- More

Back to Summary

3.5.3 Ensure RDS is disabled

Informational

Description:

The Reliable Datagram Sockets (RDS) protocol is a transport layer protocol designed to provide low-latency, high-bandwidth communications between cluster nodes. It was developed by the Oracle Corporation.

Rationale:

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install rds /bin/true
```

Assessment:

All of the following tests or sub-groups must pass:
Ensure kernel module rds is not loaded -- More
Ensure kernel module rds is not loadable -- Less

Check:	At Least One Must Pass
Command:	modprobe -n -v rds
Line Selection:	.+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/net/rds/rds.ko

Back to Summary

3.5.4 Ensure TIPC is disabled

Informational

Description:

The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communication between cluster nodes.

Rationale:

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install tipc /bin/true
```

Assessment:

All of the following tests or sub-groups must pass:
Ensure kernel module tipc is not loadable -- Less

Check:	At Least One Must Pass
Command:	modprobe -n -v tipc
Line Selection:	.+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/net/ipv4/udp_tunnel.ko
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/net/ipv6/ip6_udp_tunnel.ko
the *Std. Output* matches the regular expression **^install\s+\/bin\/true\s*$**	insmod /lib/modules/4.15.0-142-generic/kernel/net/tipc/tipc.ko

Ensure kernel module tipc is not loaded -- More

Back to Summary

3.6 Firewall Configuration

IPtables is an application that allows a system administrator to configure the IPv4 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: 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
```

Ubuntu is distributed with the UFW service which acts as a front end to iptables. The default configuration of UFW implements a configuration very similar to that recommended here. IPTables configuration allows for far more complex implementations than those listed here which may satisfy the intent of these recommendations without strictly matching the examples provided. Note: UFW may interfere with sysctl settings.

3.6.1 Ensure iptables is installed

Pass

Description:

`iptables` allows configuration of the IPv4 tables in the linux kernel and the rules stored within them. Most firewall configuration utilities operate as a front end to `iptables`.

Rationale:

iptables is required for firewall management and configuration.

Remediation:

Run the following command to install `iptables`:

```
# apt-get install iptables
```

Assessment:

Ensure package name equals 'iptables' is installed -- More

Back to Summary

3.6.2 Ensure default deny firewall policy

Pass

Description:

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Remediation:

Run the following commands to implement a default DROP policy:

```
# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
# iptables -P FORWARD DROP
```

Assessment:

All of the following tests or sub-groups must pass:
Ensure 'iptables -L' output pattern match '^Chain OUTPUT \(policy (DROP|REJECT)\)$' (string) -- More
All of the following tests or sub-groups must pass:
Ensure 'iptables -L' output pattern match '^Chain INPUT \(policy (DROP|REJECT)\)$' (string) -- More
Ensure 'iptables -L' output pattern match '^Chain FORWARD \(policy (DROP|REJECT)\)$' (string) -- More

Back to Summary

3.6.3 Ensure 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).

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:

All of the following tests or sub-groups must pass:
Ensure 'iptables -L OUTPUT -v -n' output pattern match '^\s*\S+\s+\S+\s+ACCEPT\s+all\s+--\s+*\s+lo\s+0\.0\.0\.0\/0\s+0\.0\.0\.0\/0\s*$' (string) -- Less

Check: At Least One Must Pass
Command: iptables -L OUTPUT -v -n
Line Selection: .+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^\s*\S+\s+\S+\s+ACCEPT\s+all\s+--\s+*\s+lo\s+0\.0\.0\.0\/0\s+0\.0\.0\.0\/0\s*$**	Chain OUTPUT (policy DROP 0 packets, 0 bytes)
the *Std. Output* matches the regular expression **^\s*\S+\s+\S+\s+ACCEPT\s+all\s+--\s+*\s+lo\s+0\.0\.0\.0\/0\s+0\.0\.0\.0\/0\s*$**	pkts bytes target prot opt in out source destination
the *Std. Output* matches the regular expression **^\s*\S+\s+\S+\s+ACCEPT\s+all\s+--\s+*\s+lo\s+0\.0\.0\.0\/0\s+0\.0\.0\.0\/0\s*$**	782 235K ufw-before-logging-output all -- * * 0.0.0.0/0 0.0.0.0/0
the *Std. Output* matches the regular expression **^\s*\S+\s+\S+\s+ACCEPT**	

All of the following tests or sub-groups must pass:
Ensure 'iptables -L INPUT -v -n' output pattern match '^\s*\S+\s+\S+\s+ACCEPT\s+all\s+--\s+lo\s+*\s+0\.0\.0\.0\/0\s+0\.0\.0\.0\/0\s*$' (string) -- Less

Check: At Least One Must Pass
Command: iptables -L INPUT -v -n
Line Selection: .+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^\s*\S+\s+\S+\s+ACCEPT\s+all\s+--\s+lo\s+*\s+0\.0\.0\.0\/0\s+0\.0\.0\.0\/0\s*$**	Chain INPUT (policy DROP 0 packets, 0 bytes)
the *Std. Output* matches the regular expression **^\s*\S+\s+\S+\s+ACCEPT\s+all\s+--\s+lo\s+*\s+0\.0\.0\.0\/0\s+0\.0\.0\.0\/0\s*$**	pkts bytes target prot opt in out source destination

the *Std. Output* matches the regular expression **^\s*\S+\s+\S+\s+ACCEPT\s+all\s+--\s+lo\s+*\s+0\.0\.0\.0/0\s+0\.0\.0\.0/0\s*$** 620 186K ufw-before-logging-input all -- * * 0.0.0.0/0 0.0.0.0/0

Ensure 'iptables -L INPUT -v -n' output pattern match '^\s*\S+\s+\S+\s+DROP\s+all\s+--\s+*\s+*\s+127\.0\.0\.0/8\s+0\.0\.0\.0/0\s*$' (string) -- Less

Check:	At Least One Must Pass
Command:	iptables -L INPUT -v -n
Line Selection:	.+

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **^\s*\S+\s+\S+\s+DROP\s+all\s+--\s+*\s+*\s+127\.0\.0\.0/8\s+0\.0\.0\.0/0\s*$**	Chain INPUT (policy DROP 0 packets, 0 bytes)
the *Std. Output* matches the regular expression **^\s*\S+\s+\S+\s+DROP\s+all\s+--\s+*\s+*\s+127\.0\.0\.0/8\s+0\.0\.0\.0/0\s*$**	pkts bytes target prot opt in out source destination
the *Std. Output* matches the regular expression **^\s*\S+\s+\S+\s+DROP\s+all\s+--\s+*\s+*\s+127\.0\.0\.0/8\s+0\.0\.0\.0/0\s*$**	620 186K ufw-before-logging-input all -- * * 0.0.0.0/0 0.0.0.0/0
the *Std. Output* matches the regular expression **^\s*\S+\s+\S+\s+DROP\s+all**	[illegible]

Back to Summary

3.6.5 Ensure 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.

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:

All of the following tests or sub-groups must pass:

Linux Custom Object "Firewall Rule Exists For All Open Ports" -- Less

Check:	All Must Pass
Command:	iptables -L INPUT -v -n
Line Selection:	\s+dpt:80\s+state\s+NEW\s*$

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **.+**	
Command:	iptables -L INPUT -v -n
Line Selection:	\s+dpt:53\s+state\s+NEW\s*$
CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Std. Output* matches the regular expression **.+**	
Command:	iptables -L INPUT -v -n

Linux Custom Object "Firewall Rule Exists For All Open Ports" -- Less

CIS-CAT did not expect to collect any matching items, and found 16 items.

Command: All, Line Selection: All	exists
Command: All, Line Selection: All	exists
Command: All, Line Selection: All	exists
Command: All, Line Selection: All	exists
Command: All, Line Selection: All	exists
Command: All, Line Selection: All	exists
Command: All, Line Selection: All	exists
Command: All, Line Selection: All	exists
Command: All, Line Selection: All	exists
Command: All, Line Selection: All	exists

Back to Summary

4 Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included in most distributions.

It is recommended that `rsyslog` be used for logging (with `logwatch` providing summarization) and `auditd` be used for auditing (with `aureport` providing summarization) to automatically monitor logs for intrusion attempts and other

suspicious system behavior.

In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server via an encrypted connection. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices. See the `ntpd(8)` manual page for more information on configuring NTP.

It is important that all logs described in this section be monitored on a regular basis and correlated to determine trends. A seemingly innocuous entry in one log could be more significant when compared to an entry in another log.

Note on log file permissions: There really isn't a "one size fits all" solution to the permissions on log files. Many sites utilize group permissions so that administrators who are in a defined security group, such as "wheel" do not have to elevate privileges to root in order to read log files. Also, if a third party log aggregation tool is used, it may need to have group permissions to read the log files, which is preferable to having it run setuid to root. Therefore, there are two remediation and audit steps for log file permissions. One is for systems that do not have a secured group method implemented that only permits root to read the log files (`root:root 600`). The other is for sites that do have such a setup and are designated as `root:securegrp 640` where `securegrp` is the defined security group (in some cases `wheel`).

4.1 Configure System Accounting (auditd)

System auditing, through `auditd`, allows system administrators to monitor their systems such that they can detect unauthorized access or modification of data. By default, auditd will audit SELinux AVC denials, system logins, account modifications, and authentication events. Events will be logged to `/var/log/audit/audit.log`. The recording of these events will use a modest amount of disk space on a system. If significantly more events are captured, additional on system or off system storage may need to be allocated.

The recommendations in this section implement an audit policy that produces large quantities of logged data. In some environments it can be challenging to store or process these logs and as such they are marked as Level 2 for both Servers and Workstations.

Note: For 64 bit systems that have arch as a rule parameter, you will need two rules: one for 64 bit and one for 32 bit systems. For 32 bit systems, only one rule is needed.

Note: Once all configuration changes have been made to `/etc/audit/audit.rules`, the auditd configuration must be reloaded:

```
# service auditd reload
```

4.1.1 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.

4.2 Configure Logging

Logging services should be configured to prevent information leaks and to aggregate logs on a remote server so that they can be reviewed in the event of a system compromise and ease log analysis.

4.2.1 Configure rsyslog

The `rsyslog` software is recommended as a replacement for the `syslogd` daemon and provides improvements over `syslogd`, such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

Note: This section only applies if `rsyslog` is installed on the system.

4.2.1.1 Ensure rsyslog Service is enabled Pass

Description:

Once the `rsyslog` package is installed it needs to be activated.

Rationale:

If the `rsyslog` service is not activated the system may default to the `syslogd` service or lack logging instead.

Remediation:

Run the following command to enable `rsyslog`:

```
# systemctl enable rsyslog
```

Assessment:

Any of the following tests or sub-groups may pass:
Ensure package name equals 'rsyslog' is not installed -- Less
CIS-CAT did not expect to collect any matching dpkg Packages, and found 1 item.
Package Name: rsyslog exists

Ensure standard service 'rsyslog' is enabled -- More

Back to Summary

4.2.1.3 Ensure rsyslog default file permissions 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 the /etc/rsyslog.conf and set `$FileCreateMode` to `0640` or more restrictive:

```
$FileCreateMode 0640
```

Assessment:

Any of the following tests or sub-groups may pass:
Ensure at least one file named /etc/rsyslog.conf exists and matches pattern ^\s*\$FileCreateMode\s+0[6420][40]0\s*(\s+#.*)?$ -- More
Ensure package name equals 'rsyslog' is not installed -- Less
CIS-CAT did not expect to collect any matching dpkg Packages, and found 1 item.
Package Name: rsyslog exists

Back to Summary

4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host

Fail

Description:

The `rsyslog` utility supports the ability to send logs it gathers to a remote log host running `syslogd(8)` or to receive messages from remote hosts, reducing administrative overhead.

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` file and add the following line (where *`loghost.example.com`* is the name of your central log host).

```
*.* @@loghost.example.com
```

Run the following command to restart `rsyslog`:

```
# pkill -HUP rsyslogd
```

Assessment:

Any of the following tests or sub-groups may pass:

Ensure package name equals 'rsyslog' is not installed -- Less

CIS-CAT did not expect to collect any matching dpkg Packages, and found 1 item.

Package Name: rsyslog — exists

Ensure at least one file named /etc/rsyslog.conf exists and matches pattern ^\s\.*\s+@ --** Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/rsyslog.conf
Pattern:	^\s**\.*\s+@
Match Text:	No match found

does not exist

Back to Summary

4.2.2 Configure syslog-ng

The `syslog-ng` software is recommended as a replacement for the `syslogd` daemon and provides improvements over `syslogd`, such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

Note: This section only applies if `syslog-ng` is installed on the system.

4.2.2.1 Ensure syslog-ng service is enabled

Pass

Description:

Once the `syslog-ng` package is installed it needs to be activated.

Rationale:

If the `syslog-ng` service is not activated the system may default to the `syslogd` service or lack logging instead.

Remediation:

Run the following command to enable `syslog-ng`:

```
# update-rc.d syslog-ng enable
```

Assessment:

Any of the following tests or sub-groups may pass:

Ensure standard service 'syslog-ng' is enabled -- Less

Check:	All Must Pass
Command:	systemctl is-enabled syslog-ng.service
Line Selection:	enabled

CIS-CAT Expected (At least one of)... CIS-CAT Collected...

the *Std. Output* matches the regular expression **.+**

Ensure package name equals 'syslog-ng' is not installed -- More

Back to Summary

4.2.2.3 Ensure syslog-ng default file permissions configured

Pass

Description:

syslog-ng 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 exist and have the correct permissions to ensure that sensitive `syslog-ng` data is archived and protected.

Remediation:

Edit the `/etc/syslog-ng/syslog-ng.conf` and set `perm` option to `0640` or more restrictive:

```
options { chain_hostnames(off); flush_lines(0); perm(0640); stats_freq(3600); threaded(yes); };
```

Assessment:

Any of the following tests or sub-groups may pass:

Ensure package name equals 'syslog-ng' is not installed -- More

Ensure at least one file named /etc/syslog-ng/syslog-ng.conf exists and matches pattern ^\s*options\s+\{\s*(\S+;\s*)*perm\(0[6420][40]0\);\s*(\S+;\s*)*\};\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/syslog-ng/syslog-ng.conf	does not exist
Pattern:	^\s*options\s+\{\s*(\S+;\s*)*perm\(0[6420][40]0\);\s*(\S+;\s*)*\};\s*(\s+#.*)?$	
Match Text:	No match found	

Back to Summary

4.2.3 Ensure rsyslog or syslog-ng is installed

Pass

Description:

The `rsyslog` and `syslog-ng` software are recommended replacements to the original `syslogd` daemon which provide improvements over `syslogd`, such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

Rationale:

The security enhancements of `rsyslog` and `syslog-ng` 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:

Install rsyslog or `syslog-ng` using one of the following commands:

```
# apt-get install rsyslog
# apt-get install syslog-ng
```

Assessment:

Any of the following tests or sub-groups may pass:

Ensure package name equals 'syslog-ng' is installed -- Less

CIS-CAT expected to collect at least 1 matching dpkg Package, and found 0 items.

Package Name: syslog-ng does not exist

Ensure package name equals 'rsyslog' is installed -- More

Back to Summary

4.2.4 Ensure permissions on all logfiles are configured

Fail

Description:

Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Remediation:

Run the following command to set permissions on all existing log files:

```
# chmod -R g-wx,o-rwx /var/log/*
```

Assessment:

Ensure no file(s) named .* in /var/log exists and does not have permissions ----wxrwx -- Less

File: /var/log/samba/log.	
CIS-CAT Expected...	CIS-CAT Collected...
the file's *Group Execute* to be set to **false**	false
the file's *Other Read* to be set to **false**	true
the file's *Other Execute* to be set to **false**	false
the file's *Other Write* to be set to **false**	false
the file's *Group Write* to be set to **false**	false
File: /var/log/samba/log.nmbd	
CIS-CAT Expected...	CIS-CAT Collected...
the file's *Group Execute* to be set to **false**	false

Back to Summary

5 Access, Authentication and Authorization

5.1 Configure cron

5.1.1 Ensure cron daemon is enabled

Pass

Description:

The `cron` daemon is used to execute batch jobs on the system.

Rationale:

While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and `cron` is used to execute them.

Remediation:

Run the following command to enable `cron`:

```
# systemctl enable crond
```

Assessment:

Ensure standard service 'cron' is enabled -- More

Back to Summary

5.1.2 Ensure permissions on /etc/crontab are configured

Fail

Description:

The `/etc/crontab` file is used by `cron` to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file.

Rationale:

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Remediation:

Run the following commands to set ownership and permissions on `/etc/crontab`:

```
# chown root:root /etc/crontab
# chmod og-rwx /etc/crontab
```

Assessment:

Ensure at least one file named /etc/crontab exists and is owned by 0:0 and does not have permissions ---rwxrwx -- Less

File:	/etc/crontab
CIS-CAT Expected...	CIS-CAT Collected...
the file's *Group Execute* to be set to **false**	false
the file's *Other Read* to be set to **false**	true
the file's *Group ID* to be set to **0**	0
the file's *User ID* to be set to **0**	0
the file's *Other Execute* to be set to **false**	false
the file's *Other Write* to be set to **false**	false
the file's *Group Read* to be set to **false**	true
the file's *Group Write* to be set to **false**	false

Back to Summary

5.1.3 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.

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 `/etc/cron.hourly`:

```
# chown root:root /etc/cron.hourly
# chmod og-rwx /etc/cron.hourly
```

Assessment:

Ensure at least one file named /etc/cron.hourly exists and is owned by 0:0 and does not have permissions ---rwxrwx -- Less

File:	/etc/cron.hourly
CIS-CAT Expected...	CIS-CAT Collected...
the file's *Group Execute* to be set to **false**	true
the file's *Other Read* to be set to **false**	true
the file's *Group ID* to be set to **0**	0
the file's *User ID* to be set to **0**	0
the file's *Other Execute* to be set to **false**	true
the file's *Other Write* to be set to **false**	false
the file's *Group Read* to be set to **false**	true
the file's *Group Write* to be set to **false**	false

Back to Summary

5.1.4 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.

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 `/etc/cron.daily`:

```
# chown root:root /etc/cron.daily
# chmod og-rwx /etc/cron.daily
```

Assessment:

Ensure at least one file named /etc/cron.daily exists and is owned by 0:0 and does not have permissions ---rwxrwx -- Less

File:	/etc/cron.daily
CIS-CAT Expected...	CIS-CAT Collected...
the file's *Group Execute* to be set to **false**	true
the file's *Other Read* to be set to **false**	true

the file's *Group ID* to be set to **0**	0
the file's *User ID* to be set to **0**	0
the file's *Other Execute* to be set to **false**	true
the file's *Other Write* to be set to **false**	false
the file's *Group Read* to be set to **false**	true
the file's *Group Write* to be set to **false**	false

Back to Summary

5.1.5 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.

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 `/etc/cron.weekly`:

```
# chown root:root /etc/cron.weekly
# chmod og-rwx /etc/cron.weekly
```

Assessment:

Ensure at least one file named /etc/cron.weekly exists and is owned by 0:0 and does not have permissions ---rwxrwx -- Less

File:	/etc/cron.weekly
CIS-CAT Expected...	CIS-CAT Collected...
the file's *Group Execute* to be set to **false**	true
the file's *Other Read* to be set to **false**	true
the file's *Group ID* to be set to **0**	0
the file's *User ID* to be set to **0**	0
the file's *Other Execute* to be set to **false**	true
the file's *Other Write* to be set to **false**	false
the file's *Group Read* to be set to **false**	true
the file's *Group Write* to be set to **false**	false

Back to Summary

5.1.6 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.

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 `/etc/cron.monthly`:

```
# chown root:root /etc/cron.monthly
# chmod og-rwx /etc/cron.monthly
```

Assessment:

Ensure at least one file named /etc/cron.monthly exists and is owned by 0:0 and does not have permissions ---rwxrwx -- Less

File:	/etc/cron.monthly
CIS-CAT Expected...	CIS-CAT Collected...
the file's *Group Execute* to be set to **false**	true
the file's *Other Read* to be set to **false**	true
the file's *Group ID* to be set to **0**	0
the file's *User ID* to be set to **0**	0
the file's *Other Execute* to be set to **false**	true
the file's *Other Write* to be set to **false**	false
the file's *Group Read* to be set to **false**	true
the file's *Group Write* to be set to **false**	false

Back to Summary

5.1.7 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.

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 `/etc/cron.d`:

```
# chown root:root /etc/cron.d
# chmod og-rwx /etc/cron.d
```

Assessment:

Ensure at least one file named /etc/cron.d exists and is owned by 0:0 and does not have permissions ---rwxrwx -- Less

File:	/etc/cron.d
CIS-CAT Expected...	CIS-CAT Collected...
the file's *Group Execute* to be set to **false**	true
the file's *Other Read* to be set to **false**	true
the file's *Group ID* to be set to **0**	0
the file's *User ID* to be set to **0**	0
the file's *Other Execute* to be set to **false**	true
the file's *Other Write* to be set to **false**	false
the file's *Group Read* to be set to **false**	true
the file's *Group Write* to be set to **false**	false

Back to Summary

5.1.8 Ensure at/cron is restricted to authorized users

Fail

Description:

Configure `/etc/cron.allow` and `/etc/at.allow` to allow specific users to use these services. If `/etc/cron.allow` or `/etc/at.allow` do not exist, then `/etc/at.deny` and `/etc/cron.deny` are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in `/etc/cron.allow` and `/etc/at.allow` are allowed to use at and cron. Note that 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 commands to remove `/etc/cron.deny` and `/etc/at.deny` and create and set permissions and ownership for `/etc/cron.allow` and `/etc/at.allow`:

```
# rm /etc/cron.deny
# rm /etc/at.deny
# touch /etc/cron.allow
# touch /etc/at.allow
# chmod og-rwx /etc/cron.allow
# chmod og-rwx /etc/at.allow
# chown root:root /etc/cron.allow
# chown root:root /etc/at.allow
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/at.allow exists and is owned by 0:0 and does not have permissions ---rwxrwx -- Less

CIS-CAT expected at least 1 matching file item to be collected, and found 0 items.

File: /etc/at.allow does not exist

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/cron.allow exists and is owned by 0:0 and does not have permissions ---rwxrwx -- Less

CIS-CAT expected at least 1 matching file item to be collected, and found 0 items.

File: /etc/cron.allow does not exist

All of the following tests or sub-groups must pass:

Ensure no file named /etc/at.deny exists -- More

Ensure no file named /etc/cron.deny exists -- More

Back to Summary

5.2 SSH Server Configuration

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.

Note: Once all configuration changes have been made to `/etc/ssh/sshd_config`, the sshd configuration must be reloaded:

```
# service sshd reload
```

5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured

Fail

Description:

The `/etc/ssh/sshd_config` file contains configuration specifications for `sshd`. The command below sets the owner and group of the file to root.

Rationale:

The `/etc/ssh/sshd_config` file needs to be protected from unauthorized changes by non-privileged users.

Remediation:

Run the following commands to set ownership and permissions on `/etc/ssh/sshd_config`:

```
# chown root:root /etc/ssh/sshd_config
# chmod og-rwx /etc/ssh/sshd_config
```

Assessment:

Ensure at least one file named /etc/ssh/sshd_config exists and is owned by 0:0 and does not have permissions ---rwxrwx -- Less

File:	/etc/ssh/sshd_config
CIS-CAT Expected...	CIS-CAT Collected...
the file's *Group Execute* to be set to **false**	false
the file's *Other Read* to be set to **false**	true
the file's *Group ID* to be set to **0**	0
the file's *User ID* to be set to **0**	0
the file's *Other Execute* to be set to **false**	false
the file's *Other Write* to be set to **false**	false
the file's *Group Read* to be set to **false**	true
the file's *Group Write* to be set to **false**	false

Back to Summary

5.2.2 Ensure SSH Protocol is set to 2

Pass

Description:

SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure.

Rationale:

SSH v1 suffers from insecurities that do not affect SSH v2.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Protocol 2
```

Assessment:

Ensure 'Protocol' sshd config parameter equals 2 (string) -- More

Back to Summary

5.2.3 Ensure SSH LogLevel is set to INFO

Pass

Description:

The `INFO` parameter specifies that login and logout activity will be logged.

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. `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.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LogLevel INFO
```

Assessment:

Ensure 'LogLevel' sshd config parameter equals INFO (string) -- More

Back to Summary

5.2.4 Ensure SSH X11 forwarding is disabled

Fail

Description:

The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.

Rationale:

Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
X11Forwarding no
```

Assessment:

Ensure 'X11Forwarding' sshd config parameter equals no (string) -- Less

File:	/etc/ssh/sshd_config
Pattern:	^\s*X11Forwarding\s+(\S+)\s*(?:#.*)?$
Match Text:	X11Forwarding yes

CIS-CAT Expected...	CIS-CAT Collected...
the collected item's *subexpression* to be set to **no**	yes

Back to Summary

5.2.5 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 as follows:

```
MaxAuthTries 4
```

Assessment:

Ensure 'MaxAuthTries' sshd config parameter less than or equal 4 (int) -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/ssh/sshd_config	does not exist
Pattern:	^\s*MaxAuthTries\s+(\S+)\s*(?:#.*)?$	
Match Text:	No match found	

Back to Summary

5.2.6 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 as follows:

```
IgnoreRhosts yes
```

Assessment:

Ensure 'IgnoreRhosts' sshd config parameter equals yes (string) -- More

Back to Summary

5.2.7 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. This option only applies to SSH Protocol Version 2.

Rationale:

Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, disabling the ability to use `.rhosts` files in SSH provides an additional layer of protection .

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
HostbasedAuthentication no
```

Assessment:

Ensure 'HostbasedAuthentication' sshd config parameter equals no (string) -- More

Back to Summary

5.2.8 Ensure SSH root login is disabled

Fail

Description:

The `PermitRootLogin` parameter specifies if the root user can log in using ssh(1). The default is no.

Rationale:

Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via `sudo` or `su`. This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitRootLogin no
```

Assessment:

Ensure 'PermitRootLogin' sshd config parameter equals no (string) -- Less

File:	/etc/ssh/sshd_config
Pattern:	^\s*PermitRootLogin\s+(\S+)\s*(?:#.*)?$
Match Text:	PermitRootLogin prohibit-password

CIS-CAT Expected...	CIS-CAT Collected...
the collected item's *subexpression* to be set to **no**	prohibit-password

Back to Summary

5.2.9 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 as follows:

```
PermitEmptyPasswords no
```

Assessment:

Ensure 'PermitEmptyPasswords' sshd config parameter equals no (string) -- More

Back to Summary

5.2.10 Ensure SSH PermitUserEnvironment is disabled

Fail

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 as follows:

```
PermitUserEnvironment no
```

Assessment:

Ensure 'PermitUserEnvironment' sshd config parameter equals no (string) -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/ssh/sshd_config	does not exist
Pattern:	^\s*PermitUserEnvironment\s+(\S+)\s*(?:#.*)?$	
Match Text:	No match found	

Back to Summary

5.2.11 Ensure only approved MAC algorithms are used

Fail

Description:

This variable limits the types of MAC algorithms that SSH can use during communication.

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 to set the parameter as follows:

```
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com,hmac-
sha2-512,hmac-sha2-256,umac-128@openssh.com
```

Assessment:

Ensure 'MACs' sshd config parameter pattern match ^((hmac-sha2-512-etm@openssh\.com|hmac-sha2-256-etm@openssh\.com|umac-128-etm@openssh\.com|hmac-sha2-512|hmac-sha2-256|umac-128@openssh\.com|curve25519-sha256@libssh\.org|diffie-hellman-group-exchange-sha2 -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/ssh/sshd_config	does not exist
Pattern:	^\s*MACs\s+(\S+)\s*(?:#.*)?$	
Match Text:	No match found	

Back to Summary

5.2.12 Ensure SSH Idle Timeout Interval is configured

Fail

Description:

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of ssh sessions. When the `ClientAliveInterval` variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the `ClientAliveCountMax` variable is set, `sshd` will send client alive messages at every `ClientAliveInterval` interval. When the number of consecutive client alive messages are sent with no response from the client, the `ssh` session is terminated. For example, if the `ClientAliveInterval` is set to 15 seconds and the `ClientAliveCountMax` is set to 3, the client `ssh` session will be terminated after 45 seconds of idle time.

Rationale:

Having no timeout value associated with a connection could allow an unauthorized user access to another user's `ssh` session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening..

While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for `ClientAliveCountMax` is 0. In this case, the client session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameters as follows:

```
ClientAliveInterval 300
ClientAliveCountMax 0
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'ClientAliveInterval' sshd config parameter less than or equal 300 (int) -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/ssh/sshd_config	does not exist
Pattern:	^\s*ClientAliveInterval\s+(\S+)\s*(?:#.*)?$	
Match Text:	No match found	

Ensure 'ClientAliveCountMax' sshd config parameter less than or equal 3 (int) -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/ssh/sshd_config	does not exist
Pattern:	^\s*ClientAliveCountMax\s+(\S+)\s*(?:#.*)?$	
Match Text:	No match found	

Back to Summary

5.2.13 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 as follows:

```
LoginGraceTime 60
```

Assessment:

Ensure 'LoginGraceTime' sshd config parameter less than or equal 60 (int) -- Less

File:	/etc/ssh/sshd_config
Pattern:	^\s*LoginGraceTime\s+(\S+)\s*(?:#.*)?$
Match Text:	LoginGraceTime 120

CIS-CAT Expected...	CIS-CAT Collected...
the collected item's *subexpression* to be less than or equal to **60**	120

Back to Summary

5.2.14 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 comma 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 comma 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 comma 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 comma 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 as follows:

```
AllowUsers <userlist>
AllowGroups <grouplist>
DenyUsers <userlist>
DenyGroups <grouplist>
```

Assessment:

Ensure at least one file named /etc/ssh/sshd_config exists and matches pattern ^\s*(AllowUsers|AllowGroups|DenyUsers|DenyGroups)\s+(\S+) -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/ssh/sshd_config	does not exist
Pattern:	^\s*(AllowUsers|AllowGroups|DenyUsers|DenyGroups)\s+(\S+)	
Match Text:	No match found	

Back to Summary

5.2.15 Ensure SSH warning banner is configured

Fail

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 as follows:

```
Banner /etc/issue.net
```

Assessment:

Ensure 'Banner' sshd config parameter pattern match .+ (string) -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/ssh/sshd_config	does not exist
Pattern:	^\s*Banner\s+(\S+)\s*(?:#.*)?$	
Match Text:	No match found	

Back to Summary

5.3 Configure PAM

PAM (Pluggable Authentication Modules) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the `/etc/pam.d` directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

5.3.1 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 are definitions of the `pam_pwquality.so` options.

- `try_first_pass` - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password.
- `retry=3` - Allow 3 tries before sending back a failure.

The following options are set in the `/etc/security/pwquality.conf` file:

- `minlen=14` - password must be 14 characters or more
- `dcredit=-1` - provide at least one digit
- `ucredit=-1` - provide at least one uppercase character
- `ocredit=-1` - provide at least one special character
- `lcredit=-1` - provide at least one lowercase character

The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies.

Rationale:

Strong passwords protect systems from being hacked through brute force methods.

Remediation:

Run the following command to install the pam_pwquality module:

```
apt-get install libpam-pwquality
```

Edit the `/etc/pam.d/common-passwd` file to include the appropriate options for `pam_pwquality.so` and to conform to site policy:

```
password requisite pam_pwquality.so try_first_pass retry=3
```

Edit `/etc/security/pwquality.conf` to add or update the following settings to conform to site policy:

```
minlen=14
dcredit=-1
ucredit=-1
ocredit=-1
lcredit=-1
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/security/pwquality.conf exists and matches pattern ^\s*ocredit\s*=\s*-[1-9][0-9]*\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/security/pwquality.conf	does not exist
Pattern:	^\s*ocredit\s*=\s*-[1-9][0-9]*\s*(\s+#.*)?$	
Match Text:	No match found	

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/security/pwquality.conf exists and matches pattern ^\s*ucredit\s*=\s*-[1-9][0-9]*\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/security/pwquality.conf	does not exist
Pattern:	^\s*ucredit\s*=\s*-[1-9][0-9]*\s*(\s+#.*)?$	
Match Text:	No match found	

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/security/pwquality.conf exists and matches pattern ^\s*lcredit\s*=\s*-[1-9][0-9]*\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/security/pwquality.conf
Pattern:	^\s*lcredit\s*=\s*-[1-9][0-9]*\s*(\s+#.*)?$
Match Text:	No match found

does not exist

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/security/pwquality.conf exists and matches pattern ^\s*dcredit\s*=\s*-[1-9][0-9]*\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/security/pwquality.conf
Pattern:	^\s*dcredit\s*=\s*-[1-9][0-9]*\s*(\s+#.*)?$
Match Text:	No match found

does not exist

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/security/pwquality.conf exists and matches pattern ^\s*minlen\s*=\s*(1[4-9]|[2-9][0-9]|[1-9][0-9][0-9]+)\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/security/pwquality.conf
Pattern:	^\s*minlen\s*=\s*(1[4-9]|[2-9][0-9]|[1-9][0-9][0-9]+)\s*(\s+#.*)?$
Match Text:	No match found

does not exist

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/pam.d/common-password exists and matches pattern ^\s*password\s+requisite\s+pam_pwquality\.so\s+(\S+\s+)*try_first_pass -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/pam.d/common-password
Pattern:	^\s*password\s+requisite\s+pam_pwquality\.so\s+(\S+\s+)*try_first_pass
Match Text:	No match found

does not exist

Ensure at least one file named /etc/pam.d/common-password exists and matches pattern ^\s*password\s+requisite\s+pam_pwquality\.so\s+(\S+\s+)*retry=[3210] -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/pam.d/common-password
Pattern:	^\s*password\s+requisite\s+pam_pwquality\.so\s+(\S+\s+)*retry=[3210]
Match Text:	No match found

does not exist

Back to Summary

5.3.3 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.

Note that these change only apply to accounts configured on the local system.

Remediation:

Edit the `/etc/pam.d/common-password` file to include the `remember` option and conform to site policy as shown:

```
password sufficient pam_unix.so remember=5
```

Assessment:

Ensure at least one file named /etc/pam.d/common-password exists and matches pattern ^password\s+(\S+\s+)+pam_unix\.so\s+(\S+\s+)*remember=([56789]|1-9][0-9]+) -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/pam.d/common-password	does not exist
Pattern:	^password\s+(\S+\s+)+pam_unix\.so\s+(\S+\s+)*remember=([56789]|1-9][0-9]+)	
Match Text:	No match found	

Back to Summary

5.3.4 Ensure password hashing algorithm is SHA-512

Pass

Description:

The commands below change password encryption from `md5` to `sha512` (a much stronger hashing algorithm). All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.

Rationale:

The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

Note that these change only apply to accounts configured on the local system.

Remediation:

Edit the `/etc/pam.d/common-password` file to include the `sha512` option for `pam_unix.so` as shown:

```
password [success=1 default=ignore] pam_unix.so sha512
```

Assessment:

Ensure at least one file named /etc/pam.d/common-password exists and matches pattern ^password\s+(\S+\s+)+pam_unix\.so\s+(\S+\s+)*sha512 -- More

Back to Summary

5.4 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

5.4.1 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.

5.4.1.1 Ensure password expiration is 90 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. It is recommended that the `PASS_MAX_DAYS` parameter be set to less than or equal to 90 days.

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.

Remediation:

Set the `PASS_MAX_DAYS` parameter to `90` in `/etc/login.defs`:

```
PASS_MAX_DAYS 90
```

Modify user parameters for all users with a password set to match:

```
# chage --maxdays 90 <user>
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/login.defs exists and matches pattern ^\s*PASS_MAX_DAYS\s+(90|[1-8][0-9]|[1-9])\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/login.defs	does not exist
Pattern:	^\s*PASS_MAX_DAYS\s+(90|[1-8][0-9]|[1-9])\s*(\s+#.*)?$	
Match Text:	No match found	

Linux Custom Object "Ensure no users with a Password have password expiration over 90 days" -- Less

Check:	None May Pass	
User:	student	
CIS-CAT Expected...		CIS-CAT Collected...
the *Password Life (days)* to be greater than **90**		99999
User:	patcpett	
CIS-CAT Expected...		CIS-CAT Collected...
the *Password Life (days)* to be greater than **90**		99999
User:	dunnxter	
CIS-CAT Expected...		CIS-CAT Collected...
the *Password Life (days)* to be greater than **90**		99999

Back to Summary

5.4.1.2 Ensure minimum days between password changes is 7 or more

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 7 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 7 in `/etc/login.defs`:

```
PASS_MIN_DAYS 7
```

Modify user parameters for all users with a password set to match:

```
# chage --mindays 7 <user>
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/login.defs exists and matches pattern ^\s*PASS_MIN_DAYS\s+([789]|[1-9][0-9]+)\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/login.defs	does not exist
Pattern:	^\s*PASS_MIN_DAYS\s+([789]|[1-9][0-9]+)\s*(\s+#.*)?$	
Match Text:	No match found	

Linux Custom Object "Ensure no users with a Password have password change minimum under 7 days" -- Less

Check:	None May Pass	
User:	student	
CIS-CAT Expected...		CIS-CAT Collected...
the *Password Minimum Age* to be less than **7**		0
User:	patcpett	
CIS-CAT Expected...		CIS-CAT Collected...
the *Password Minimum Age* to be less than **7**		0
User:	dunnxter	
CIS-CAT Expected...		CIS-CAT Collected...
the *Password Minimum Age* to be less than **7**		0

Back to Summary

5.4.1.3 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:

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/login.defs exists and matches pattern ^\s*PASS_WARN_AGE\s+([789][[1-9][0-9]+)\s*(\s+#.*)?$ -- More

Linux Custom Object "Ensure no users with a Password have password expiration warning under 7 days" -- More

Back to Summary

5.4.1.4 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:

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/default/useradd exists and matches pattern ^\s*INACTIVE\s*=\s*(30|[1-2][0-9]|[1-9])\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/default/useradd	does not exist
Pattern:	^\s*INACTIVE\s*=\s*(30|[1-2][0-9]|[1-9])\s*(\s+#.*)?$	
Match Text:	No match found	

Linux Custom Object "Ensure no users with a Password have password inactivation over 30 days" -- More

Back to Summary

5.4.2 Ensure system accounts are non-login

Fail

Description:

There are a number of accounts provided with Ubuntu 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, Ubuntu sets 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 `/sbin/nologin`. This prevents the account from potentially being used to run any commands.

Remediation:

Set the shell for any accounts returned by the audit script to `/usr/sbin/nologin`:

```
# usermod -s /usr/sbin/nologin <user>
```

The following script will automatically set all user shells required to `/usr/sbin/nologin` and lock the `sync`, `shutdown`, and `halt` users:

```
#!/bin/bash

for user in `awk -F: '($3 < 1000) {print $1 }' /etc/passwd`; do
if [ $user != "root" ]; then
usermod -L $user
if [ $user != "sync" ] && [ $user != "shutdown" ] && [ $user != "halt" ]; then
usermod -s /usr/sbin/nologin $user
fi
fi
done
```

Assessment:

Linux Custom Object "System Accounts Disabled" -- Less

Check:	None May Pass	
User:	daemon	
CIS-CAT Expected...		CIS-CAT Collected...
the *User ID* to be less than **1000**		1
the *Login Shell* to not be set to **/usr/sbin/nologin**		/usr/sbin/nologin
User:	bin	
CIS-CAT Expected...		CIS-CAT Collected...
the *User ID* to be less than **1000**		2
the *Login Shell* to not be set to **/usr/sbin/nologin**		/usr/sbin/nologin
User:	sys	

Back to Summary

5.4.3 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:

Linux Custom Object "Default Group Set For root User" -- More

Back to Summary

5.4.4 Ensure default user umask is 027 or more restrictive

Fail

Description:

The default `umask` determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the `umask` command into the standard shell configuration files (`.profile`, `.bashrc`, etc.) in their home directories.

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:

Edit the `/etc/bash.bashrc` and `/etc/profile` files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:

```
umask 027
```

Assessment:

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/profile exists and does not match pattern ^\s*umask\s+[01234567](0[7654321]|[7654321][654321])\s*(\s+#.*)?$ -- More

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/profile exists and matches pattern ^\s*umask\s+[01234567][2367]7\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/profile	does not exist
Pattern:	^\s*umask\s+[01234567][2367]7\s*(\s+#.*)?$	
Match Text:	No match found	

All of the following tests or sub-groups must pass:

Ensure at least one file named /etc/bash.bashrc exists and matches pattern ^\s*umask\s+[01234567][2367]7\s*(\s+#.*)?$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/bash.bashrc	does not exist
Pattern:	^\s*umask\s+[01234567][2367]7\s*(\s+#.*)?$	
Match Text:	No match found	

Ensure at least one file named /etc/bash.bashrc exists and does not match pattern ^\s*umask\s+[01234567](0[7654321]|[7654321][654321])\s*(\s+#.*)?$ -- More

Back to Summary

5.6 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 the wheel group to execute `su`.

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:

Add the following line to the `/etc/pam.d/su` file:

```
auth required pam_wheel.so use_uid
```

Create a comma separated list of users in the wheel statement in the `/etc/group` file:

```
wheel:x:10:root,<user list>
```

Assessment:

Ensure at least one file named /etc/pam.d/su exists and matches pattern ^\s*auth\s+required\s+pam_wheel.so\s+use_uid\s*$ -- Less

CIS-CAT expected at least 1 matching text file content item to be collected, and found 0 items.

File:	/etc/pam.d/su	does not exist
Pattern:	^\s*auth\s+required\s+pam_wheel.so\s+use_uid\s*$	
Match Text:	No match found	

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.

6.1.2 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 command to set permissions on `/etc/passwd`:

```
# chown root:root /etc/passwd
# chmod 644 /etc/passwd
```

Assessment:

Ensure at least one file named /etc/passwd exists and is owned by 0:0 and has permissions rw-r--r-- and does not have permissions --x-wx-wx SUID SGID sticky -- More

Back to Summary

6.1.3 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 the one following commands to set permissions on `/etc/shadow`:

```
# chown root:shadow /etc/shadow
# chmod o-rwx,g-wx /etc/shadow
```

Assessment:

Ensure at least one file named /etc/shadow exists and is owned by 0:42 and does not have permissions --x-wxrwx SUID SGID sticky -- More

Back to Summary

6.1.4 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 command to set permissions on `/etc/group`:

```
# chown root:root /etc/group
# chmod 644 /etc/group
```

Assessment:

Ensure at least one file named /etc/group exists and is owned by 0:0 and has permissions rw-r--r-- and does not have permissions --x-wx-wx SUID SGID sticky -- More

Back to Summary

6.1.5 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 the the following commands to set permissions on `/etc/gshadow`:

```
# chown root:shadow /etc/gshadow
# chmod o-rwx,g-rw /etc/gshadow
```

Assessment:

Ensure at least one file named /etc/gshadow exists and is owned by 0:42 and does not have permissions --x-wxrwx SUID SGID sticky -- More

Back to Summary

6.1.6 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 command to set permissions on `/etc/passwd-`:

```
# chown root:root /etc/passwd-
# chmod 600 /etc/passwd-
```

Assessment:

Ensure at least one file named /etc/passwd- exists and is owned by 0:0 and does not have permissions --xrwxrwx SUID SGID sticky -- More

Back to Summary

6.1.7 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 the following command to set permissions on `/etc/shadow-`:

```
# chown root:root /etc/shadow-
# chmod 600 /etc/shadow-
```

Assessment:

Ensure at least one file named /etc/shadow- exists and is owned by 0:0 and does not have permissions --xrwxrwx SUID SGID sticky -- More

Back to Summary

6.1.8 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 command to set permissions on `/etc/group-`:

```
# chown root:root /etc/group-
# chmod 600 /etc/group-
```

Assessment:

Ensure at least one file named /etc/group- exists and is owned by 0:0 and does not have permissions --xrwxrwx SUID SGID sticky -- More

Back to Summary

6.1.9 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 the following command to set permissions on `/etc/gshadow-`:

```
# chown root:root /etc/gshadow-
# chmod 600 /etc/gshadow-
```

Assessment:

Ensure at least one file named /etc/gshadow- exists and is owned by 0:0 and does not have permissions --xrwxrwx SUID SGID sticky -- More

Back to Summary

6.1.10 Ensure no world writable files exist

Unknown

Description:

Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the `chmod(2)` man page for more information.

Rationale:

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

Remediation:

Removing write access for the "other" category (`chmod o-w <filename>`) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.

Assessment:

Ensure no world writable files exist -- More

Back to Summary

6.1.11 Ensure no unowned files or directories exist

Unknown

Description:

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Remediation:

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Assessment:

Ensure no unowned files or directories exist -- More

Back to Summary

6.1.12 Ensure no ungrouped files or directories exist

Unknown

Description:

Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Remediation:

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Assessment:

Ensure no ungrouped files or directories exist -- More

Back to Summary

6.2 User and Group Settings

This section provides guidance on securing aspects of the users and groups.

6.2.1 Ensure password fields are not empty

Fail

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:

Ensure usernames pattern match .+ have shadow parameter password pattern match .+ (string) -- Less

Check:	All Must Pass	
User:	root	
CIS-CAT Expected...		CIS-CAT Collected...
the *Encrypted Password* matches the regular expression **.+**		!
User:	daemon	
CIS-CAT Expected...		CIS-CAT Collected...
the *Encrypted Password* matches the regular expression **.+**		*
User:	bin	
CIS-CAT Expected...		CIS-CAT Collected...
the *Encrypted Password* matches the regular expression **.+**		*

Back to Summary

6.2.2 Ensure no legacy "+" entries exist in /etc/passwd

Pass

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Remediation:

Remove any legacy '+' entries from `/etc/passwd` if they exist.

Assessment:

Ensure at least one file named /etc/passwd exists and does not match pattern ^\+: -- More

Back to Summary

6.2.3 Ensure no legacy "+" entries exist in /etc/shadow

Pass

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Remediation:

Remove any legacy '+' entries from `/etc/shadow` if they exist.

Assessment:

Ensure at least one file named /etc/shadow exists and does not match pattern ^\+: -- More

Back to Summary

6.2.4 Ensure no legacy "+" entries exist in /etc/group

Pass

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Remediation:

Remove any legacy '+' entries from `/etc/group` if they exist.

Assessment:

Ensure at least one file named /etc/group exists and does not match pattern ^\+: -- More

Back to Summary

6.2.5 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:

Ensure at least one file named /etc/passwd exists and does not match pattern ^(?!root:)[^:]*:[^:]*:0 -- More

Back to Summary

6.2.6 Ensure root PATH Integrity

Fail

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:

All of the following tests or sub-groups must pass:

Linux Custom Object "Root Path Directories Are Owned By UID 0 And Not Writable By Group Or Other" -- Less

CIS-CAT expected every collected file item to exist on the target system, and found 6 items.

File:	/usr/local/sbin	exists
File:	/usr/local/bin	exists
File:	/usr/sbin	exists
File:	/usr/bin	exists
File:	/sbin	exists
File:	/bin	exists
File:	/snap/bin	does not exist

All of the following tests or sub-groups must pass:

Linux Custom Object "Root Path Does Not Include "."" -- More

Linux Custom Object "Root Path Does Not Include """ -- More

Back to Summary

6.2.7 Ensure all users' home directories exist

Fail

Description:

Users can be defined in `/etc/passwd` without a home directory or with a home directory that does not actually exist.

Rationale:

If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

Remediation:

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

Assessment:

Linux Custom Object "All User Home Directories Exist" -- Less

CIS-CAT expected every collected file item to exist on the target system, and found 36 items.

File:	/usr/sbin	exists
File:	/bin	exists
File:	/dev	exists
File:	/usr/games	exists
File:	/var/cache/man	exists
File:	/var/spool/lpd	does not exist
File:	/var/mail	exists
File:	/var/spool/news	does not exist
File:	/var/spool/uucp	does not exist
File:	/bin	exists

Back to Summary

6.2.8 Ensure users' home directories permissions are 750 or more restrictive

Fail

Description:

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

Rationale:

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Remediation:

Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

Assessment:

Linux Custom Object "No User Home Directories Have Permissions ----w-rwx" -- Less

File:	/usr/sbin	
CIS-CAT Expected...		CIS-CAT Collected...
the file's *Other Read* to be set to **false**		true
the file's *Other Execute* to be set to **false**		true
the file's *Other Write* to be set to **false**		false
the file's *Group Write* to be set to **false**		false
File:	/bin	
CIS-CAT Expected...		CIS-CAT Collected...
the file's *Other Read* to be set to **false**		true
the file's *Other Execute* to be set to **false**		true

Back to Summary

6.2.9 Ensure users own their home directories

Pass

Description:

The user home directory is space defined for the particular user to set local environment variables and to store personal files.

Rationale:

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

Remediation:

Change the ownership of any home directories that are not owned by the defined user to the correct user.

Assessment:

Ensure 'cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do if [$uid -ge 1000 -a -d "$dir" -a $user != "nfsnobody"]; then owner=$(stat -L -c "%U" "$dir"); if ["$owner" != "$user"]; then echo "The home directory ($dir) -- More

Back to Summary

6.2.10 Ensure users' dot files are not group or world writable

Pass

Description:

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

Rationale:

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

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.

Assessment:

Linux Custom Object "No User Dot Files Have Permissions ----w--w-" -- More

Back to Summary

6.2.11 Ensure no users have .forward files

Pass

Description:

The `.forward` file specifies an email address to forward the user's mail to.

Rationale:

Use of the `.forward` file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The `.forward` file also poses a risk as it can be used to execute commands that may perform unintended actions.

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.forward` files and determine the action to be taken in accordance with site policy.

Assessment:

Linux Custom Object "No User Home Directories Contain .forward Files" -- More

Back to Summary

6.2.12 Ensure no users have .netrc files

Pass

Description:

The `.netrc` file contains data for logging into a remote host for file transfers via FTP.

Rationale:

The `.netrc` file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over `.netrc` files from other systems which could pose a risk to those systems.

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.netrc` files and determine the action to be taken in accordance with site policy.

Assessment:

Linux Custom Object "No User Home Directories Contain .netrc Files" -- More

Back to Summary

6.2.13 Ensure users' .netrc Files are not group or world accessible

Pass

Description:

While the system administrator can establish secure permissions for users' `.netrc` files, the users can easily override these.

Rationale:

`.netrc` files may contain unencrypted passwords that may be used to attack other systems.

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.netrc` file permissions and determine the action to be taken in accordance with site policy.

Assessment:

Linux Custom Object "No User .netrc Files Have Permissions ---rwxrwx" -- More

Back to Summary

6.2.14 Ensure no users have .rhosts files

Pass

Description:

While no `.rhosts` files are shipped by default, users can easily create them.

Rationale:

This action is only meaningful if `.rhosts` support is permitted in the file `/etc/pam.conf`. Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.rhosts` files

and determine the action to be taken in accordance with site policy.

Assessment:

Linux Custom Object "No User Home Directories Contain .rhost Files" -- More

Back to Summary

6.2.15 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:

Linux Custom Object "All Groups In /etc/passwd Exist In /etc/group" -- More

Back to Summary

6.2.16 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:

Linux Custom Object "Check For Duplicate UIDs" -- More

Back to Summary

6.2.17 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:

Linux Custom Object "Check For Duplicate GIDs" -- More

Back to Summary

6.2.18 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:

Linux Custom Object "Check For Duplicate User Names" -- More

Back to Summary

6.2.19 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:

Linux Custom Object "Check For Duplicate Group Names" -- More

Back to Summary

6.2.20 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:

Remove all users from the shadow group, and change the primary group of any users with shadow as their primary group.

Assessment:

Linux Custom Object "Shadow Group is Empty" -- More

Back to Summary

⇧