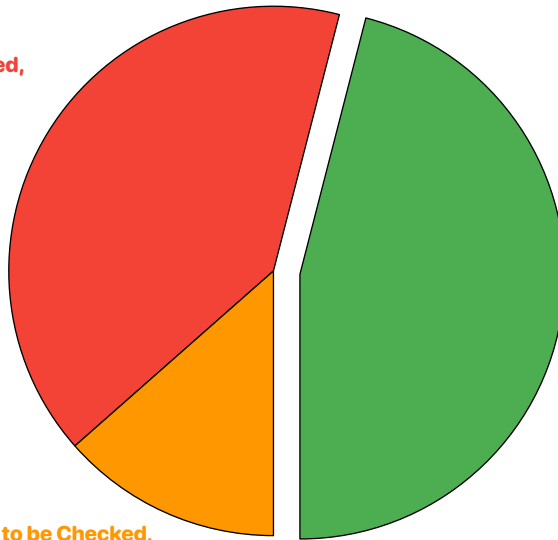


Result of CIS Distribution Independent Linux Benchmark v2.0.0

109 tests passed, where 104 were Scored.

This system's Score is 44%

96 of 237 tests (40.506%) Failed,
which is 40.506% of all tests



109 of 237 tests (45.992%) Passed,
which is 45.992% of all tests

32 of 237 tests (13.502%) are to be Checked,
which is 13.502% of all tests

Start Time (UTC): 2021-8-2 5:49:44

Start Time (Local): 2021-8-2 15:49:44

Finish Time (UTC): 2021-8-2 5:50:10

Finish Time (Local): 2021-8-2 15:50:10

Performed 237 tests in 26.417 seconds

Auditor Description

Included Controls

Excluded Controls

Scoring Level

Both Level 1 and 2

Score

Both Scored and Not Scored

Platform

Verbosity

False

Index of Results

1.1.1.1	cramfs cannot be mounted	PASS
1.1.1.2	freevxfs cannot be mounted	PASS
1.1.1.3	jffs2 cannot be mounted	PASS
1.1.1.4	hfs cannot be mounted	PASS
1.1.1.5	hfsplus cannot be mounted	PASS
1.1.1.6	squashfs mount status undetermined	PASS
1.1.1.7	udf mount status undetermined	PASS
1.1.1.8	vfat is mounted	CHEK
1.1.2	/tmp is configured	PASS
1.1.3	nodev is not set on /tmp	FAIL
1.1.4	nosuid is set on /tmp	PASS
1.1.5	noexec is not set on /tmp	FAIL
1.1.6	/var is not configured	FAIL
1.1.7	/var/tmp is not configured	FAIL
1.1.8	nodev is not set on /var/tmp	FAIL
1.1.9	nodev is not set on /var/tmp	FAIL
1.1.10	noexec is not set on /var/tmp	FAIL
1.1.11	/var/log is not configured	FAIL
1.1.12	/var/log/audit is not configured	FAIL
1.1.13	/home is not configured	FAIL
1.1.14	nodev is not set on /home	FAIL
1.1.15	nodev is set on /dev/shm	PASS
1.1.16	nosuid is set on /dev/shm	PASS
1.1.17	noexec is not set on /dev/shm	FAIL
1.1.18	No mounted media found	PASS
1.1.19	No mounted media found	PASS
1.1.20	No mounted media found	PASS
1.1.21	sticky bit set on w-w directories	PASS
1.1.22	automounting could not be checked	PASS
1.1.23	usb-storage cannot be mounted	PASS
1.2.1	package configuration not checked (ind distro)	CHEK
1.2.2	GPG keys source not checked (ind distro)	CHEK

1.3.1	AIDE not checked (ind distro)	CHEK
1.3.2	No AIDE cron jobs scheduled	FAIL
1.4.1	bootloader permits group and others	FAIL
1.4.2	bootloader password not checked	CHEK
1.4.3	auth not required for single user mode	FAIL
1.4.4	interactive boot not checked	CHEK
1.5.1	core dumps not restricted	FAIL
1.5.2	XD/NX support is enabled	PASS
1.5.3	ASLR not enabled	FAIL
1.5.4	prelink not checked (ind distro)	CHEK
1.6.1.1	SELinux or AppArmor not checked (ind distro)	CHEK
1.6.2.1	SELinux not disabled boot-config	PASS
1.6.2.2	SELinux state is not enforcing	FAIL
1.6.2.3	SELinux policy is not configured	FAIL
1.6.2.4	SETroubleshoot not checked (ind distro)	CHEK
1.6.2.5	mcstrans not checked (ind distro)	CHEK
1.6.2.6	no unconfined daemons exist	PASS
1.6.3.1	AppArmor not disabled boot-config	PASS
1.6.3.2	all AppArmor Profiles are enforcing	PASS
1.7.1.1	no message of the day	CHEK
1.7.1.2	login banner contains sensitive info	FAIL
1.7.1.3	remote banner contains sensitive info	FAIL
1.7.1.4	/etc/motd not found	CHEK
1.7.1.5	/etc/issue permissions configured	PASS
1.7.1.6	/etc/issue.net permissions configured	PASS
1.7.2	GDM not found	CHEK
1.8	software not checked (ind distro)	CHEK
2.1.1	chargen is not present	PASS
2.1.2	daytime is not present	PASS
2.1.3	discard is not present	PASS
2.1.4	echo is not present	PASS
2.1.5	time is not present	PASS
2.1.6	rsh services not present	PASS
2.1.7	talk server not present	PASS

2.1.8	telnet server not present	PASS
2.1.9	tftp server not present	PASS
2.1.10	xinetd not found	PASS
2.2.1.1	time sync not checked (ind distro)	CHEK
2.2.1.2	ntp not configured	FAIL
2.2.1.3	remote server not configured	FAIL
2.2.1.4	system clock not synchronized	FAIL
2.2.2	X Window System not checked (ind distro)	CHEK
2.2.3	avahi-daemon not found	PASS
2.2.4	cups not found	PASS
2.2.5	dhcpcd not found	PASS
2.2.6	slapd not found	PASS
2.2.7	npc and rpcbind are disabled	PASS
2.2.8	named not found	PASS
2.2.9	vsftpd not found	PASS
2.2.10	httpd not found	PASS
2.2.11	dovecot not found	PASS
2.2.12	smb not found	PASS
2.2.13	squid not found	PASS
2.2.14	snmpd not found	PASS
2.2.15	mta is local only	PASS
2.2.16	rsyncd not found	PASS
2.2.17	ypserv not found	PASS
2.3.1	NIS Client not checked (ind distro)	CHEK
2.3.2	rsh Client not checked (ind distro)	CHEK
2.3.3	talk Client not checked (ind distro)	CHEK
2.3.4	telnet Client not checked (ind distro)	CHEK
2.3.5	LDAP Client not checked (ind distro)	CHEK
3.1.1	IP forwarding disabled	PASS
3.1.2	packet redirect sending is disabled	PASS
3.2.1	source routed packets are not accepted	PASS
3.2.2	ICMP redirects not accepted	PASS
3.2.3	secure ICMP redirects not accepted	PASS
3.2.4	suspicious packets are logged	PASS

3.2.5	ipv4 broadcasts not ignored	FAIL
3.2.6	bogus ICMP responses ignored	PASS
3.2.7	Reverse Path Filtering enabled	PASS
3.2.8	TCP SYN Cookies enabled	PASS
3.2.9	ipv6 all ra accepted	FAIL
3.3.1	TCP Wrappers not checked (ind distro)	CHEK
3.3.2	/etc/hosts.allow not configured	FAIL
3.3.3	/etc/hosts.deny not configured	FAIL
3.3.4	/etc/hosts.allow permissions configured	PASS
3.3.5	/etc/hosts.deny permissions configured	PASS
3.4.1	dccp cannot be mounted	PASS
3.4.2	sctp cannot be mounted	PASS
3.4.3	rds cannot be mounted	PASS
3.4.4	tipc cannot be mounted	PASS
3.5.1.1	IPv6 default no deny policy	FAIL
3.5.1.2	IPv6 input loopback no config	FAIL
3.5.1.3	IPv6 Table contains no config	FAIL
3.5.1.4	open ports no firewall rule	FAIL
3.5.2.1	no default deny firewall	FAIL
3.5.2.2	fw input loopback no config	FAIL
3.5.2.3	iptables contains no config	FAIL
3.5.2.4	open ports no firewall rule	FAIL
3.5.3	iptables not checked (ind distro)	CHEK
3.6	wireless interfaces disabled	PASS
3.7	IPv6 enabled	FAIL
4.1.1.1	audit log storage size is configured	PASS
4.1.1.2	system disabled when audit logs full	PASS
4.1.1.3	audit logs automatically deleted	FAIL
4.1.2	auditd not checked (ind distro)	CHEK
4.1.3	auditd runlevel S02 not found	FAIL
4.1.4	processes prior to auditd not audited	FAIL
4.1.5	events modifying date and time not coll	FAIL
4.1.6	events modifying u/g info not coll	FAIL
4.1.7	events modifying system's n/w env not coll	FAIL

4.1.8	events modifying system's MAC not coll	FAIL
4.1.9	login and logout events not collected	FAIL
4.1.10	session initiation info not collected	FAIL
4.1.11	access control mod events not coll	FAIL
4.1.12	unauthorized file access not coll	FAIL
4.1.13	privileged commands not collected	FAIL
4.1.14	successful fs mounts not collected	FAIL
4.1.15	unlink, rename *.rules events not coll	FAIL
4.1.16	changes to sudoers not collected	FAIL
4.1.17	sudolog not collected	FAIL
4.1.18	kernel module not monitored	FAIL
4.1.19	audit configuration is mutable	FAIL
4.2.1.1	rsyslog not checked (ind distro)	CHEK
4.2.1.2	rsyslog runlevel S02 not found	FAIL
4.2.1.3	logging is configured	CHEK
4.2.1.4	rsyslog file permissions configured	PASS
4.2.1.5	rsyslog does not sends logs	FAIL
4.2.1.6	rsyslog messages not config	FAIL
4.2.2.1	journald does not send logs to rsyslog	FAIL
4.2.2.2	journald not compress large log files	FAIL
4.2.2.3	journald does not write logfiles	FAIL
4.2.3	logfiles permissions not configured	FAIL
4.3	lograte is configured	CHEK
5.1.1	cron daemon not found	FAIL
5.1.2	perms on /etc/crontab not configured	FAIL
5.1.3	perms on /etc/cron.hourly not configured	FAIL
5.1.4	perms on /etc/cron.daily not configured	FAIL
5.1.5	perms on /etc/cron.weekly not configured	FAIL
5.1.6	perms on /etc/cron.monthly not configured	FAIL
5.1.7	perms on /etc/cron.d not configured	FAIL
5.1.8	/etc/at.deny exists	FAIL
5.2.1	perms on sshd_config not configured	FAIL
5.2.2	SSH private host keys perms config	PASS
5.2.3	SSH public host keys perms config	PASS

5.2.4	SSH Protocol not 2	FAIL
5.2.5	SSH LogLevel is appropriate	PASS
5.2.6	SSH X11 forwarding not disabled	FAIL
5.2.7	SSH MaxAuthTries is more than 4	FAIL
5.2.8	SSH IgnoreRhosts is disabled	FAIL
5.2.9	SSH HBA is enabled	FAIL
5.2.10	SSH root login is enabled	FAIL
5.2.11	SSH PermitEmptyPasswords is enabled	FAIL
5.2.12	SSH PermitUserEnvironment is enabled	FAIL
5.2.13	SSH only strong Ciphers are used	PASS
5.2.14	SSH only strong MAC algorithms are used	PASS
5.2.15	SSH only strong Key Exchange algorithms are used	PASS
5.2.16	SSH ClientAliveInterval more than 300	FAIL
5.2.17	SSH LoginGraceTime is 60	PASS
5.2.18	SSH access is not limited	FAIL
5.2.19	SSH warning banner is not configured	FAIL
5.2.20	SSH PAM is enabled	PASS
5.2.21	SSH AllowTcpForwarding is enabled	FAIL
5.2.22	SSH MaxStartups is configured	CHEK
5.2.23	SSH MaxSessions is set to 10	CHEK
5.3.1	password creation req not found	FAIL
5.3.2	failed password lockout configured	CHEK
5.3.3	password reuse not limited	FAIL
5.3.4	password hashing algorithm is SHA-512	CHEK
5.4.1.1	password expiration not 365 days or less	FAIL
5.4.1.2	password changes not 7 days or more	FAIL
5.4.1.3	password change warning gt 7 days	PASS
5.4.1.4	inactive password lock more than 30 days	FAIL
5.4.1.5	last password change date in past	PASS
5.4.2	system accounts are secured	PASS
5.4.3	root account GID is 0	PASS
5.4.4	umask not found in bashrc	FAIL
5.4.5	shell timeout not in bashrc	FAIL
5.5	root login is restricted to system	PASS

5.6	access to su command not restricted	FAIL
6.1.1	system file perms not checked (ind distro)	CHEK
6.1.2	/etc/passwd permissions configured	PASS
6.1.3	/etc/shadow permissions configured	PASS
6.1.4	/etc/group permissions configured	PASS
6.1.5	/etc/gshadow permissions configured	PASS
6.1.6	/etc/passwd- permits group and others	FAIL
6.1.7	/etc/shadow- permissions configured	PASS
6.1.8	/etc/group- permissions configured	PASS
6.1.9	/etc/gshadow- permissions configured	PASS
6.1.10	world writable files does not exist	PASS
6.1.11	no unowned files or directories exist	PASS
6.1.12	no ungrouped files or directories exist	PASS
6.1.13	SUID executables found	FAIL
6.1.14	SGID executables found	FAIL
6.2.1	password fields are not empty	PASS
6.2.2	no legacy "+" entries exist in /etc/passwd	PASS
6.2.3	no legacy "+" entries exist in /etc/shadow	PASS
6.2.4	no legacy "+" entries exist in /etc/group	PASS
6.2.5	root is the only UID 0 account	PASS
6.2.6	writable dir in root's executable path	FAIL
6.2.7	all users' home directories exist	PASS
6.2.8	Group or world-writable home directories	FAIL
6.2.9	users own their home directories	PASS
6.2.10	users' . files not group or world-writable	PASS
6.2.11	no users have .forward files	PASS
6.2.12	no users have .netrc files	PASS
6.2.13	users' .netrc not group or world accessible	PASS
6.2.14	no users have .rhosts files	PASS
6.2.15	all groups in passwd exist in group	PASS
6.2.16	no duplicate UIDs exist	PASS
6.2.17	no duplicate GIDs exist	PASS
6.2.18	no duplicate user names exist	PASS
6.2.19	no duplicate group names exist	PASS

6.2.20 **users not assigned to shadow group** **PASS**

1.1.1.1

Ensure mounting of cramfs filesystems is disabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message cramfs cannot be mounted

Time Taken 0.05118298530578613 seconds

Explanation:

install /bin/true

1.1.1.2

Ensure mounting of freevxfs filesystems is disabled

Scored

Level 1 Server

Level 1 Workstation

Result	PASS
Message	freevxfs cannot be mounted
Time Taken	0.06055426597595215 seconds

Explanation:

install /bin/true

1.1.1.3

Ensure mounting of jffs2 filesystems is disabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message jffs2 cannot be mounted

Time Taken 0.0668036937713623 seconds

Explanation:

install /bin/true

1.1.1.4

Ensure mounting of hfs filesystems is disabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message hfs cannot be mounted

Time Taken 0.06933808326721191 seconds

Explanation:

install /bin/true

1.1.1.5

Ensure mounting of hfsplus filesystems is disabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message hfsplus cannot be mounted

Time Taken 0.04512500762939453 seconds

Explanation:

install /bin/true

1.1.1.6

Ensure mounting of squashfs filesystems is disabled

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

squashfs mount status undetermined

Time Taken

0.07855868339538574 seconds

Explanation:

1.1.1.7

Ensure mounting of udf filesystems is disabled

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

udf mount status undetermined

Time Taken

0.07344937324523926 seconds

Explanation:

udf

118784 0

crc_itu_t

16384 1 udf

1.1.1.8

Ensure mounting of FAT filesystems is limited

Not Scored

Level 2 Server

Level 2 Workstation

Result

CHEK

Message

vfat is mounted

Time Taken

0.020717144012451172 seconds

Explanation:

UUID=C4E4-E7F8

/boot/efi

vfat

umask=0077

0 1

1.1.2

Ensure /tmp is configured

Scored
Level 1 Server
Level 1 Workstation

Result **PASS**

Message /tmp is configured

Time Taken 0.02659296989440918 seconds

Explanation:

/usr/tmpDSK on /tmp type tmpfs (rw,nosuid,relatime,loop)

1.1.3

Ensure nodev option set on /tmp partition

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message nodev is not set on /tmp

Time Taken 0.07898402214050293 seconds

Explanation:

mount | grep -E '\s/tmp\s' returned the following

/usr/tmpDSK on /tmp type tmpfs (rw,nosuid,relatime,loop)

1.1.4

Ensure nosuid option set on /tmp partition

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message nosuid is set on /tmp

Time Taken 0.06789565086364746 seconds

Explanation:

```
mount | grep -E '\s/tmp\s' | grep -v nosuid did not return anything
```

1.1.5

Ensure noexec option set on /tmp partition

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message noexec is not set on /tmp

Time Taken 0.08628296852111816 seconds

Explanation:

`mount | grep -E '\s/tmp\s' | grep -v noexec` returned the following

`/usr/tmpDSK on /tmp type tmpfs (rw,nosuid,relatime,loop)`

1.1.6

Ensure separate partition exists for /var

Scored

Level 2 Server

Level 2 Workstation

Result FAIL

Message /var is not configured

Time Taken 0.037688493728637695 seconds

Explanation:

mount | grep -E '\s/var\s' did not return any result

1.1.7

Ensure separate partition exists for /var/tmp

Scored

Level 2 Server

Level 2 Workstation

Result FAIL

Message /var/tmp is not configured

Time Taken 0.03805184364318848 seconds

Explanation:

mount | grep /var/tmp did not return any result

1.1.8

Ensure nodev option set on /var/tmp partition

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message nodev is not set on /var/tmp

Time Taken 0.048723459243774414 seconds

Explanation:

/var/tmp does not exist. nodev cannot be set on a partition that does not exist

1.1.9

Ensure nosuid option set on /var/tmp partition

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message nodev is not set on /var/tmp

Time Taken 0.0492091178894043 seconds

Explanation:

/var/tmp does not exist. nosuid cannot be set on a partition that does not exist

1.1.10

Ensure noexec option set on /var/tmp partition

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message noexec is not set on /var/tmp

Time Taken 0.03858804702758789 seconds

Explanation:

/var/tmp does not exist. noexec cannot be set on a partition that does not exist

1.1.11

Ensure separate partition exists for /var/log

Scored

Level 2 Server

Level 2 Workstation

Result FAIL

Message /var/log is not configured

Time Taken 0.025725603103637695 seconds

Explanation:

mount | grep /var/log did not return any result

1.1.12

Ensure separate partition exists for /var/log/audit

Scored

Level 2 Server

Level 2 Workstation

Result FAIL

Message /var/log/audit is not configured

Time Taken 0.040662288665771484 seconds

Explanation:

mount | grep /var/log/audit did not return any result

1.1.13

Ensure separate partition exists for /home

Scored

Level 2 Server

Level 2 Workstation

Result FAIL

Message /home is not configured

Time Taken 0.04345512390136719 seconds

Explanation:

mount | grep /home did not return any result

1.1.14

Ensure nodev option set on /home partition

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message nodev is not set on /home

Time Taken 0.042873382568359375 seconds

Explanation:

/home does not exist. nodev cannot be set on a partition that does not exist

1.1.15

Ensure nodev option set on /dev/shm partition

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message nodev is set on /dev/shm

Time Taken 0.0618901252746582 seconds

Explanation:

mount | grep -E '\s/dev/shm\s' | grep -v nodev did not return any thing

1.1.16

Ensure nosuid option set on /dev/shm partition

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message nosuid is set on /dev/shm

Time Taken 0.07674026489257812 seconds

Explanation:

mount | grep -E '\s/dev/shm\s' | grep -v nosuid did not return anything

1.1.17

Ensure noexec option set on /dev/shm partition

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message noexec is not set on /dev/shm

Time Taken 0.09308385848999023 seconds

Explanation:

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

1.1.18

Ensure nodev option set on removable media partitions

Not Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message No mounted media found

Time Taken 0.04043436050415039 seconds

Explanation:

mount | grep -e '/media/' returned no result

1.1.19

Ensure nosuid option set on removable media partitions

Not Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message No mounted media found

Time Taken 0.04518461227416992 seconds

Explanation:

mount | grep -e '/media/' returned no result

1.1.20

Ensure noexec option set on removable media partitions

Not Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message No mounted media found

Time Taken 0.04280424118041992 seconds

Explanation:

mount | grep -e '/media/' returned no result

1.1.21

Ensure sticky bit is set on all world-writable directories

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message sticky bit set on w-w directories

Time Taken **1.5746395587921143 seconds**

Explanation:

running `df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{ }' find '{ }' -xdev -type d \(-perm -0002 -a ! -perm -1000 \) 2>/dev/null` confirms that all world writable directories have the sticky variable set

1.1.22

Disable Automounting

Scored
Level 1 Server
Level 2 Workstation

Result	PASS
Message	automounting could not be checked
Time Taken	0.06213808059692383 seconds

Explanation:

Failed to get unit file state for autofs.service: No such file or directory

1.1.23

Disable USB Storage

Scored
Level 1 Server
Level 2 Workstation

Result	PASS
Message	usb-storage cannot be mounted
Time Taken	0.0763859748840332 seconds

Explanation:

modprobe: FATAL: Module usb-storage not found in directory /lib/modules/5.4.0-1055-azure

1.2.1

Ensure package manager repositories are configured (distro specific)

Not Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

package configuration not checked (ind distro)

Time Taken

9.918212890625e-05 seconds

Explanation:

Distribution was not specified

1.2.2

Ensure GPG keys are configured (distro specific)

Not Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

GPG keys source not checked (ind distro)

Time Taken

2.5033950805664062e-05 seconds

Explanation:

Distribution was not specified

1.3.1

Ensure AIDE is installed (distro specific)

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

AIDE not checked (ind distro)

Time Taken

1.9073486328125e-05 seconds

Explanation:

Distribution was not specified

1.3.2

Ensure filesystem integrity is regularly checked

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message No AIDE cron jobs scheduled

Time Taken 0.03460407257080078 seconds

Explanation:

grep -r aide /etc/cron.* /etc/crontab returned the following

no crontab for root

1.4.1

Ensure permissions on bootloader config are configured (bootloader specific)

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message bootloader permits group and others

Time Taken **0.03319048881530762 seconds**

Explanation:

Access: (0444/-r--r--r--) Uid: (0/ root) Gid: (0/ root)

Access: 2021-08-02 15:39:55.445747854 +1000

1.4.2

Ensure bootloader password is set (bootloader specific)

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

bootloader password not checked

Time Taken

0.053177833557128906 seconds

Explanation:

1.4.3

Ensure authentication required for single user mode

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message auth not required for single user mode

Time Taken 0.02324843406677246 seconds

Explanation:

grep ^root:[*\!]: /etc/shadow returned the following

1.4.4

Ensure interactive boot is not enabled (bootloader specific)

Not Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

interactive boot not checked

Time Taken

0.02148747444152832 seconds

Explanation:

grep "^PROMPT_FOR_CONFIRM=" /etc/sysconfig/boot returned the following

grep: /etc/sysconfig/boot: No such file or directory

1.5.1

Ensure core dumps are restricted

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message core dumps not restricted

Time Taken 0.07750082015991211 seconds

Explanation:

Following are configured properly

/etc/security/limits.d/core_dump.conf:* hard core 0

fs.suid_dumpable = 2

/etc/sysctl.conf:fs.suid_dumpable=0

/etc/sysctl.d/99-sysctl.conf:fs.suid_dumpable=0

Following are configured improperly

1.5.2

Ensure XD/NX support is enabled

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

XD/NX support is enabled

Time Taken

0.2571566104888916 seconds

Explanation:

Aug 02 15:10:43 ubuntu kernel: NX (Execute Disable) protection: active

Aug 02 15:21:57 pkrvm0juwrm8arp kernel: NX (Execute Disable) protection: active

1.5.3

Ensure address space layout randomization (ASLR) is enabled

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message ASLR not enabled

Time Taken 0.04770612716674805 seconds

Explanation:

Following are configured properly

kernel.randomize_va_space = 2

Following are configured improperly

1.5.4

Ensure prelink is disabled (distro specific)

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

prelink not checked (ind distro)

Time Taken

0.00011038780212402344 seconds

Explanation:

Distribution was not specified

1.6.1.1

Ensure SELinux or AppArmor are installed (distro specific)

Scored

Level 2 Server

Level 2 Workstation

Result

CHEK

Message

SELinux or AppArmor not checked (ind distro)

Time Taken

2.9802322387695312e-05 seconds

Explanation:

Distribution was not specified

1.6.2.1

Ensure SELinux is not disabled in bootloader configuration

Scored

Level 2 Server

Level 2 Workstation

Result PASS

Message SELinux not disabled boot-config

Time Taken 0.023011445999145508 seconds

Explanation:

```
kernel /boot/vmlinuz-4.15.0-151-generic root=LABEL=cloud
img-rootfs ro console=hvc0
```

```
kernel /boot/vmlinuz-4.15.0-151-generic root=LABEL=cloud
img-rootfs ro single
```

1.6.2.2

Ensure the SELinux state is enforcing

Scored

Level 2 Server

Level 2 Workstation

Result **FAIL**

Message SELinux state is not enforcing

Time Taken 0.018541812896728516 seconds

Explanation:

Following are configured properly

Following are configured improperly

grep: /etc/selinux/config: No such file or directory

/bin/bash: sestatus: command not found

1.6.2.3

Ensure SELinux policy is configured

Scored
Level 2 Server
Level 2 Workstation

Result **FAIL**

Message SELinux policy is not configured

Time Taken 0.0512852668762207 seconds

Explanation:

Following are configured properly

Following are configured improperly

grep: /etc/selinux/config: No such file or directory

/bin/bash: sestatus: command not found

1.6.2.4

Ensure SETroubleshoot is not installed (distro specific)

Scored

Level 2 Server

N/A

Result

CHEK

Message

SETroubleshoot not checked (ind distro)

Time Taken

7.081031799316406e-05 seconds

Explanation:

Distribution was not specified

1.6.2.5

Ensure the MCS Translation Service (mcstrans) is not installed (distro specific)

Scored

Level 2 Server

Level 2 Workstation

Result

CHEK

Message

mcstrans not checked (ind distro)

Time Taken

2.3365020751953125e-05 seconds

Explanation:

Distribution was not specified

1.6.2.6

Ensure no unconfined daemons exist

Scored

Level 2 Server

Level 2 Workstation

Result **PASS**

Message no unconfined daemons exist

Time Taken 0.059533119201660156 seconds

Explanation:

```
ps -eZ | grep -E "initrc" | grep -E -v -w "tr|ps|grep|bash|awk" |  
tr ':' ' ' | awk '{ print $NF }' returned nothing
```

1.6.3.1

Ensure AppArmor is not disabled in bootloader configuration

Scored

Level 2 Server

Level 2 Workstation

Result PASS

Message AppArmor not disabled boot-config

Time Taken 0.026812314987182617 seconds

Explanation:

```
kernel /boot/vmlinuz-4.15.0-151-generic root=LABEL=cloud
img-rootfs ro console=hvc0
```

```
kernel /boot/vmlinuz-4.15.0-151-generic root=LABEL=cloud
img-rootfs ro single
```

1.6.3.2

Ensure all AppArmor Profiles are enforcing

Scored

Level 2 Server

Level 2 Workstation

Result

PASS

Message

all AppArmor Profiles are enforcing

Time Taken

0.6112985610961914 seconds

Explanation:

apparmor module is loaded.

15 profiles are loaded.

15 profiles are in enforce mode.

/sbin/dhclient

/usr/bin/lxc-start

/usr/bin/man

/usr/lib/NetworkManager/nm-dhcp-client.action

/usr/lib/NetworkManager/nm-dhcp-helper

/usr/lib/connman/scripts/dhclient-script

/usr/lib/snapd/snap-confine

/usr/lib/snapd/snap-confine//mount-namespace-capture-helper

/usr/sbin/tcpdump

lxc-container-default

lxc-container-default-cgns

lxc-container-default-with-mounting

lxc-container-default-with-nesting

man_filter

man_groff

0 profiles are in complain mode.

0 processes have profiles defined.

0 processes are in enforce mode.

0 processes are in complain mode.

0 processes are unconfined but have a profile defined.

1.7.1.1

Ensure message of the day is configured properly

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

no message of the day

Time Taken

0.020101070404052734 seconds

Explanation:

cat: /etc/motd: No such file or directory

1.7.1.2

Ensure local login warning banner is configured properly

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message login banner contains sensitive info

Time Taken 0.05194520950317383 seconds

Explanation:

Following OS [or] patch level information were found in the local login banner

Ubuntu 18.04.5 LTS \n \1

1.7.1.3

Ensure remote login warning banner is configured properly

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message remote banner contains sensitive info

Time Taken 0.0527651309967041 seconds

Explanation:

Following OS [or] patch level information were found in the remote login banner

#####

#This system is the property of Accenture, and is to be used in accordance #

#with applicable Accenture Policies. Unauthorized access or activity is a #

#violation of Accenture Policies and may be a violation of law. Use of this #

#system constitutes consent to monitoring or unauthorized use, in accordance #

#with Accenture Policies, local laws, and regulations. Unauthorized use may #

#result in penalties including, but not limited to, reprimand, dismissal, #

#financial penalties, and legal action.

#

#####

1.7.1.4

Ensure permissions on /etc/motd are configured

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

/etc/motd not found

Time Taken

0.024477005004882812 seconds

Explanation:

stat /etc/motd | grep Access did not return anything

stat: cannot stat '/etc/motd': No such file or directory

1.7.1.5

Ensure permissions on /etc/issue are configured

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message /etc/issue permissions configured

Time Taken **0.03155255317687988 seconds**

Explanation:

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

Access: 2021-08-02 15:11:03.590703300 +1000

1.7.1.6

Ensure permissions on /etc/issue.net are configured

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message /etc/issue.net permissions configured

Time Taken 0.024985551834106445 seconds

Explanation:

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

Access: 2021-08-02 15:23:05.506273117 +1000

1.7.2

Ensure GDM login banner is configured

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

GDM not found

Time Taken

0.02034616470336914 seconds

Explanation:

cat /etc/gdm3/greeter.dconf-defaults did not return anything

cat: /etc/gdm3/greeter.dconf-defaults: No such file or directory

1.8

Ensure updates, patches, and additional security software are installed (distro specific)

Not Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

software not checked (ind distro)

Time Taken

7.843971252441406e-05 seconds

Explanation:

Distribution was not specified

2.1.1

Ensure chargen services are not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message chargen is not present

Time Taken 0.021674156188964844 seconds

Explanation:

grep -R "^chargen" /etc/inetd.* returned the following

grep: /etc/inetd.*: No such file or directory

2.1.2

Ensure daytime services are not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message daytime is not present

Time Taken 0.020288467407226562 seconds

Explanation:

grep -R "^daytime" /etc/inetd.* returned the following

grep: /etc/inetd.*: No such file or directory

2.1.3

Ensure discard services are not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message discard is not present

Time Taken 0.029462337493896484 seconds

Explanation:

grep -R "^discard" /etc/inetd.* returned the following

grep: /etc/inetd.*: No such file or directory

2.1.4

Ensure echo services are not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message echo is not present

Time Taken 0.3175804615020752 seconds

Explanation:

grep -R "^echo" /etc/inetd.* returned the following

2.1.5

Ensure time services are not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message time is not present

Time Taken 0.02297520637512207 seconds

Explanation:

grep -R "^time" /etc/inetd.* returned the following

grep: /etc/inetd.*: No such file or directory

2.1.6

Ensure rsh server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message rsh services not present

Time Taken 0.06716132164001465 seconds

Explanation:

grep: /etc/inetd.*: No such file or directory

grep: /etc/inetd.*: No such file or directory

grep: /etc/inetd.*: No such file or directory

2.1.7

Ensure talk server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

talk server not present

Time Taken

0.04357790946960449 seconds

Explanation:

grep: /etc/inetd.*: No such file or directory

grep: /etc/inetd.*: No such file or directory

2.1.8

Ensure telnet server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message telnet server not present

Time Taken 0.022593259811401367 seconds

Explanation:

grep -R "^telnet" /etc/inetd.* returned the following

grep: /etc/inetd.*: No such file or directory

2.1.9

Ensure tftp server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message tftp server not present

Time Taken **0.02735447883605957 seconds**

Explanation:

grep -R "^tftp" /etc/inetd.* returned the following

grep: /etc/inetd.*: No such file or directory

2.1.10

Ensure xinetd is not enabled

Scored
Level 1 Server
Level 1 Workstation

Result **PASS**

Message xinetd not found

Time Taken 0.034219980239868164 seconds

Explanation:

systemctl is-enabled xinetd returned the following

Failed to get unit file state for xinetd.service: No such file or directory

2.2.1.1

Ensure time synchronization is in use (distro specific)

Not Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

time sync not checked (ind distro)

Time Taken

7.62939453125e-05 seconds

Explanation:

Distribution was not specified

2.2.1.2

Ensure ntp is configured

Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	ntp not configured
Time Taken	0.02588677406311035 seconds
Explanation:	
grep: /etc/ntp.conf: No such file or directory	

2.2.1.3

Ensure chrony is configured

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message remote server not configured

Time Taken 0.023194074630737305 seconds

Explanation:

grep -E "^(server|pool)" /etc/chrony.conf returned the following

grep: /etc/chrony.conf: No such file or directory

2.2.1.4

Ensure systemd-timesyncd is configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message system clock not synchronized

Time Taken **25.089691162109375 seconds**

Explanation:

enabled

Ensure that the NTP servers, NTP FallbackNTP servers, and RootDistanceMaxSec listed are in accordance with local policy

This file is part of systemd.

#

systemd is free software; you can redistribute it and/or modify it

under the terms of the GNU Lesser General Public License as published by

the Free Software Foundation; either version 2.1 of the License, or

(at your option) any later version.

#

Entries in this file show the compile time defaults.

You can change settings by editing this file.

Defaults can be restored by simply deleting this file.

#

See timesyncd.conf(5) for details.

[Time]

#NTP=

#FallbackNTP=ntp.ubuntu.com

#RootDistanceMaxSec=5

#PollIntervalMinSec=32

#PollIntervalMaxSec=2048

Failed to query server: Failed to activate service 'org.freedesktop.timedate1': timed out (service_start_timeout=25000ms)

2.2.2

Ensure X Window System is not installed (distro specific)

Scored

Level 1 Server

N/A

Result

CHEK

Message

X Window System not checked (ind distro)

Time Taken

5.8650970458984375e-05 seconds

Explanation:

Distribution was not specified

2.2.3

Ensure Avahi Server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message avahi-daemon not found

Time Taken **0.035651445388793945 seconds**

Explanation:

systemctl is-enabled avahi-daemon returned the following

Failed to get unit file state for avahi-daemon.service: No such file or directory

2.2.4

Ensure CUPS is not enabled

Scored
Level 1 Server
Level 2 Workstation

Result **PASS**

Message cups not found

Time Taken 0.035294532775878906 seconds

Explanation:

systemctl is-enabled cups returned the following

Failed to get unit file state for cups.service: No such file or directory

2.2.5

Ensure DHCP Server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message dhcpd not found

Time Taken **0.05756998062133789 seconds**

Explanation:

systemctl is-enabled dhcpd returned the following

Failed to get unit file state for dhcpd.service: No such file or directory

2.2.6

Ensure LDAP server is not enabled

Scored
Level 1 Server
Level 1 Workstation

Result **PASS**

Message slapd not found

Time Taken 0.035588979721069336 seconds

Explanation:

systemctl is-enabled slapd returned the following

Failed to get unit file state for slapd.service: No such file or directory

2.2.7

Ensure NFS and RPC are not enabled

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message npc and rpcbind are disabled

Time Taken 0.054424285888671875 seconds

Explanation:

systemctl is-enabled nfs returned the following

Failed to get unit file state for nfs.service: No such file or directory

systemctl is-enabled rpcbind returned the following

Failed to get unit file state for rpcbind.service: No such file or directory

2.2.8

Ensure DNS Server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message named not found

Time Taken 0.030738353729248047 seconds

Explanation:

systemctl is-enabled named returned the following

Failed to get unit file state for named.service: No such file or directory

2.2.9

Ensure FTP Server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message vsftpd not found

Time Taken 0.031537532806396484 seconds

Explanation:

systemctl is-enabled vsftpd returned the following

Failed to get unit file state for vsftpd.service: No such file or directory

2.2.10

Ensure HTTP server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message httpd not found

Time Taken 0.03307914733886719 seconds

Explanation:

systemctl is-enabled httpd returned the following

Failed to get unit file state for httpd.service: No such file or directory

2.2.11

Ensure IMAP and POP3 server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message dovecot not found

Time Taken 0.029710054397583008 seconds

Explanation:

systemctl is-enabled dovecot returned the following

Failed to get unit file state for dovecot.service: No such file or directory

2.2.12

Ensure Samba is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message smb not found

Time Taken 0.032431602478027344 seconds

Explanation:

systemctl is-enabled smb returned the following

Failed to get unit file state for smb.service: No such file or directory

2.2.13

Ensure HTTP Proxy Server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message squid not found

Time Taken 0.027208566665649414 seconds

Explanation:

systemctl is-enabled squid returned the following

Failed to get unit file state for squid.service: No such file or directory

2.2.14

Ensure SNMP Server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message snmpd not found

Time Taken 0.0324552059173584 seconds

Explanation:

systemctl is-enabled snmpd returned the following

Failed to get unit file state for snmpd.service: No such file or directory

2.2.15

Ensure mail transfer agent is configured for local-only mode

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message mta is local only

Time Taken 0.024671554565429688 seconds

Explanation:

ss -lntu | grep -E ':25\s' | grep -E -v '\s(127.0.0.1|::1):25\s'
returned the following

2.2.16

Ensure rsync service is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message rsyncd not found

Time Taken 0.03319215774536133 seconds

Explanation:

systemctl is-enabled rsyncd returned the following

Failed to get unit file state for rsyncd.service: No such file or directory

2.2.17

Ensure NIS Server is not enabled

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message ypserv not found

Time Taken 0.03061676025390625 seconds

Explanation:

systemctl is-enabled ypserv returned the following

Failed to get unit file state for ypserv.service: No such file or directory

2.3.1

Ensure NIS Client is not installed (distro specific)

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

NIS Client not checked (ind distro)

Time Taken

9.369850158691406e-05 seconds

Explanation:

Distribution was not specified

2.3.2

Ensure rsh client is not installed (distro specific)

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

rsh Client not checked (ind distro)

Time Taken

3.0994415283203125e-05 seconds

Explanation:

Distribution was not specified

2.3.3

Ensure talk client is not installed (distro specific)

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

talk Client not checked (ind distro)

Time Taken

1.9073486328125e-05 seconds

Explanation:

Distribution was not specified

2.3.4

Ensure telnet client is not installed (distro specific)

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

telnet Client not checked (ind distro)

Time Taken

1.52587890625e-05 seconds

Explanation:

Distribution was not specified

2.3.5

Ensure LDAP client is not installed (distro specific)

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

LDAP Client not checked (ind distro)

Time Taken

3.314018249511719e-05 seconds

Explanation:

Distribution was not specified

3.1.1

Ensure IP forwarding is disabled

Scored
Level 1 Server
Level 1 Workstation

Result PASS

Message IP forwarding disabled

Time Taken 0.07557797431945801 seconds

Explanation:

net.ipv6.conf.all.forwarding = 0

/etc/sysctl.conf:#net.ipv6.conf.all.forwarding=1

/etc/sysctl.d/99-sysctl.conf:#net.ipv6.conf.all.forwarding=1

3.1.2

Ensure packet redirect sending is disabled

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message packet redirect sending is disabled

Time Taken **0.06659126281738281 seconds**

Explanation:

net.ipv4.conf.default.send_redirects = 0

/etc/sysctl.conf:net.ipv4.conf.default.send_redirects=0

/etc/sysctl.d/99-sysctl.conf:net.ipv4.conf.default.send_redirects=0

3.2.1

Ensure source routed packets are not accepted

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message source routed packets are not accepted

Time Taken 0.1368100643157959 seconds

Explanation:

net.ipv6.conf.all.accept_source_route = 0

/etc/sysctl.conf:#net.ipv6.conf.all.accept_source_route = 0

/etc/sysctl.conf:net.ipv6.conf.all.accept_source_route=0

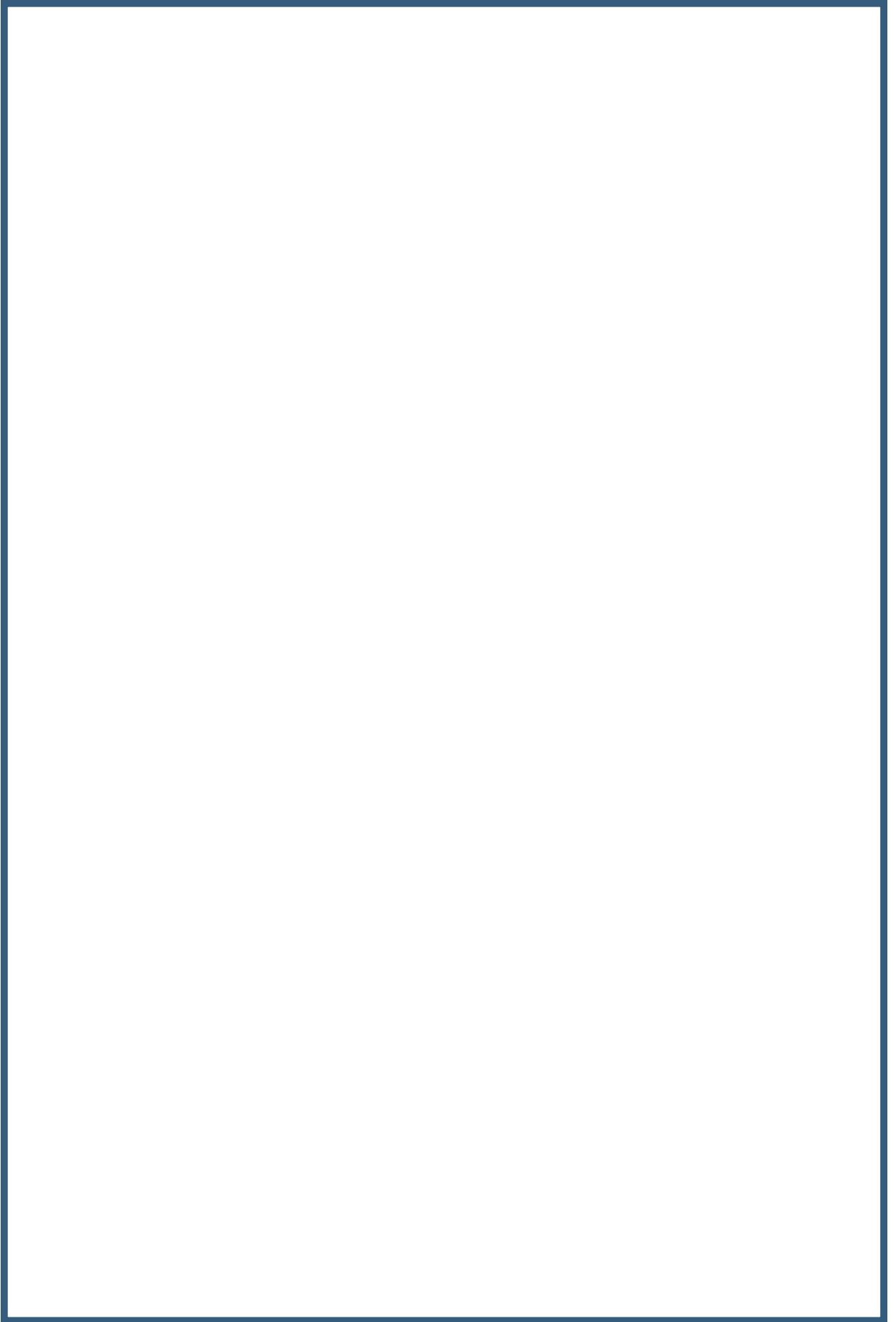
/etc/sysctl.d/99-sysctl.conf:#net.ipv6.conf.all.accept_source_route = 0

/etc/sysctl.d/99-sysctl.conf:net.ipv6.conf.all.accept_source_route=0

net.ipv6.conf.default.accept_source_route = 0

/etc/sysctl.conf:net.ipv6.conf.default.accept_source_route=0

/etc/sysctl.d/99-sysctl.conf:net.ipv6.conf.default.accept_source_route=0



3.2.2

Ensure ICMP redirects are not accepted

Scored

Level 1 Server

Level 1 Workstation

Result	PASS
Message	ICMP redirects not accepted
Time Taken	0.14217710494995117 seconds

Explanation:

net.ipv6.conf.all.accept_redirects = 0

/etc/sysctl.conf:#net.ipv6.conf.all.accept_redirects = 0

/etc/sysctl.conf:net.ipv6.conf.all.accept_redirects=0

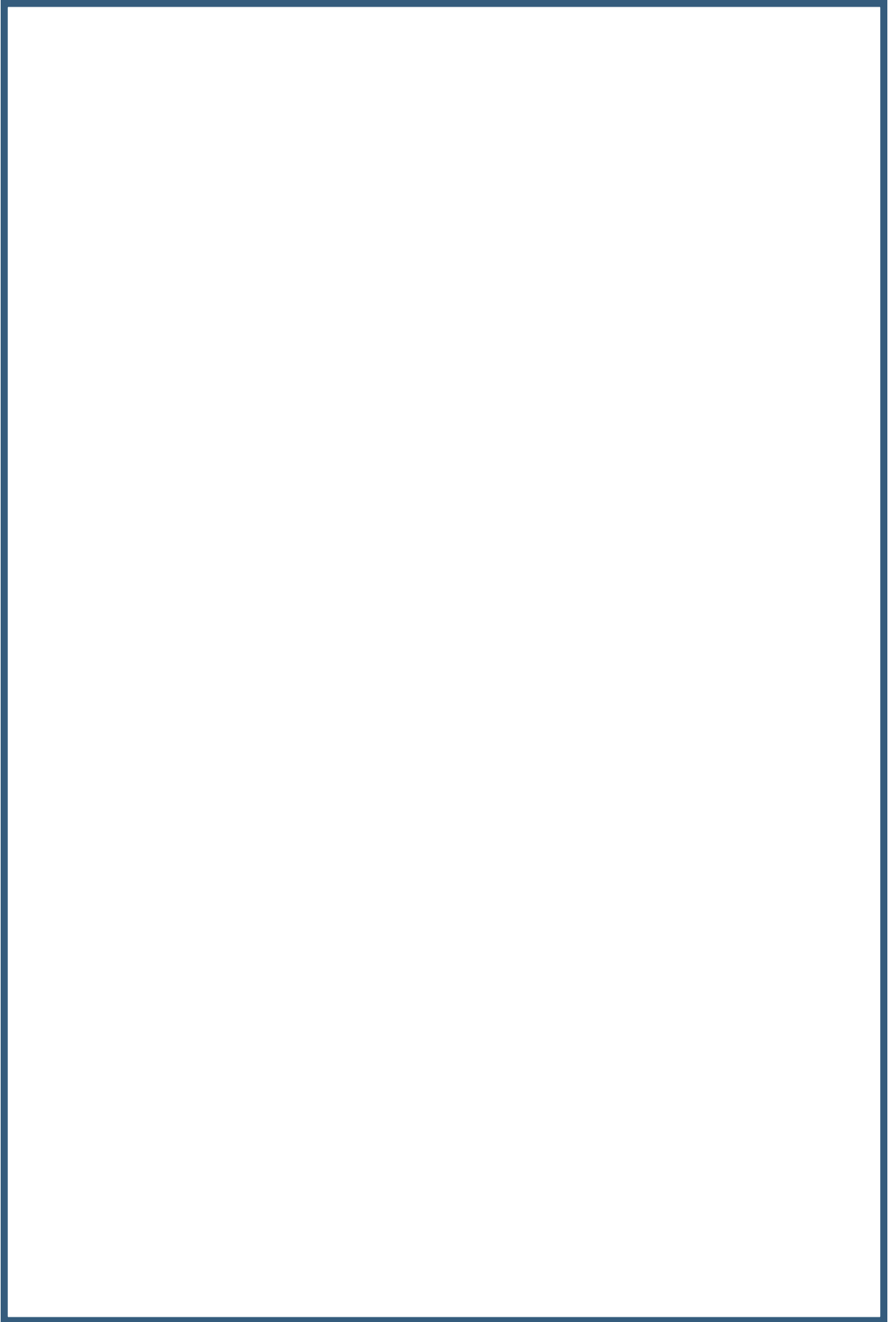
/etc/sysctl.d/99-sysctl.conf:#net.ipv6.conf.all.accept_redirects = 0

/etc/sysctl.d/99-sysctl.conf:net.ipv6.conf.all.accept_redirects=0

net.ipv6.conf.default.accept_redirects = 0

/etc/sysctl.conf:net.ipv6.conf.default.accept_redirects=0

/etc/sysctl.d/99-sysctl.conf:net.ipv6.conf.default.accept_redirects=0



3.2.3

Ensure secure ICMP redirects are not accepted

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message secure ICMP redirects not accepted

Time Taken **0.06770873069763184 seconds**

Explanation:

net.ipv4.conf.default.secure_redirects = 0

/etc/sysctl.conf:net.ipv4.conf.default.secure_redirects=0

/etc/sysctl.d/99-sysctl.conf:net.ipv4.conf.default.secure_redirects=0

3.2.4

Ensure suspicious packets are logged

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

suspicious packets are logged

Time Taken

0.07508063316345215 seconds

Explanation:

net.ipv4.conf.default.log_martians = 1

/etc/sysctl.conf:net.ipv4.conf.default.log_martians=1

/etc/sysctl.d/99-sysctl.conf:net.ipv4.conf.default.log_martians=1

3.2.5

Ensure broadcast ICMP requests are ignored

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message ipv4 broadcasts not ignored

Time Taken 0.016107797622680664 seconds

Explanation:

`net.ipv4.icmp_echo_ignore_broadcasts = 0`

3.2.6

Ensure bogus ICMP responses are ignored

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

bogus ICMP responses ignored

Time Taken

0.03471708297729492 seconds

Explanation:

net.ipv4.icmp_ignore_bogus_error_responses = 1

/etc/sysctl.conf:net.ipv4.icmp_ignore_bogus_error_responses=1

/etc/sysctl.d/99-sysctl.conf:net.ipv4.icmp_ignore_bogus_error_responses=1

3.2.7

Ensure Reverse Path Filtering is enabled

Scored

Level 1 Server

Level 1 Workstation

Result	PASS
Message	Reverse Path Filtering enabled
Time Taken	0.08310914039611816 seconds

Explanation:

net.ipv4.conf.default.rp_filter = 1

/etc/sysctl.conf:#net.ipv4.conf.default.rp_filter=1

/etc/sysctl.conf:net.ipv4.conf.default.rp_filter=1

/etc/sysctl.d/10-network-security.conf:net.ipv4.conf.default.rp_filter=1

/etc/sysctl.d/99-sysctl.conf:#net.ipv4.conf.default.rp_filter=1

/etc/sysctl.d/99-sysctl.conf:net.ipv4.conf.default.rp_filter=1

3.2.8

Ensure TCP SYN Cookies is enabled

Scored
Level 1 Server
Level 1 Workstation

Result PASS

Message TCP SYN Cookies enabled

Time Taken 0.040493011474609375 seconds

Explanation:

net.ipv4.tcp_syncookies = 1

/etc/sysctl.conf:#net.ipv4.tcp_syncookies=1

/etc/sysctl.conf:net.ipv4.tcp_syncookies=1

/etc/sysctl.d/10-network-security.conf:net.ipv4.tcp_syncookies=1

/etc/sysctl.d/99-sysctl.conf:#net.ipv4.tcp_syncookies=1

/etc/sysctl.d/99-sysctl.conf:net.ipv4.tcp_syncookies=1

3.2.9

Ensure IPv6 router advertisements are not accepted

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message ipv6 all ra accepted

Time Taken 0.016718149185180664 seconds

Explanation:

net.ipv6.conf.all.accept_ra = 1

3.3.1

Ensure TCP Wrappers is installed (distro specific)

Not Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

TCP Wrappers not checked (ind distro)

Time Taken

6.794929504394531e-05 seconds

Explanation:

Distribution was not specified

3.3.2

Ensure /etc/hosts.allow is configured

Not Scored
Level 1 Server
Level 1 Workstation

Result **FAIL**

Message /etc/hosts.allow not configured

Time Taken 0.019950151443481445 seconds

Explanation:

/etc/hosts.allow: list of hosts that are allowed to access the system.

See the manual pages hosts_access(5) and hosts_options(5).

#

Example: ALL: LOCAL @some_netgroup

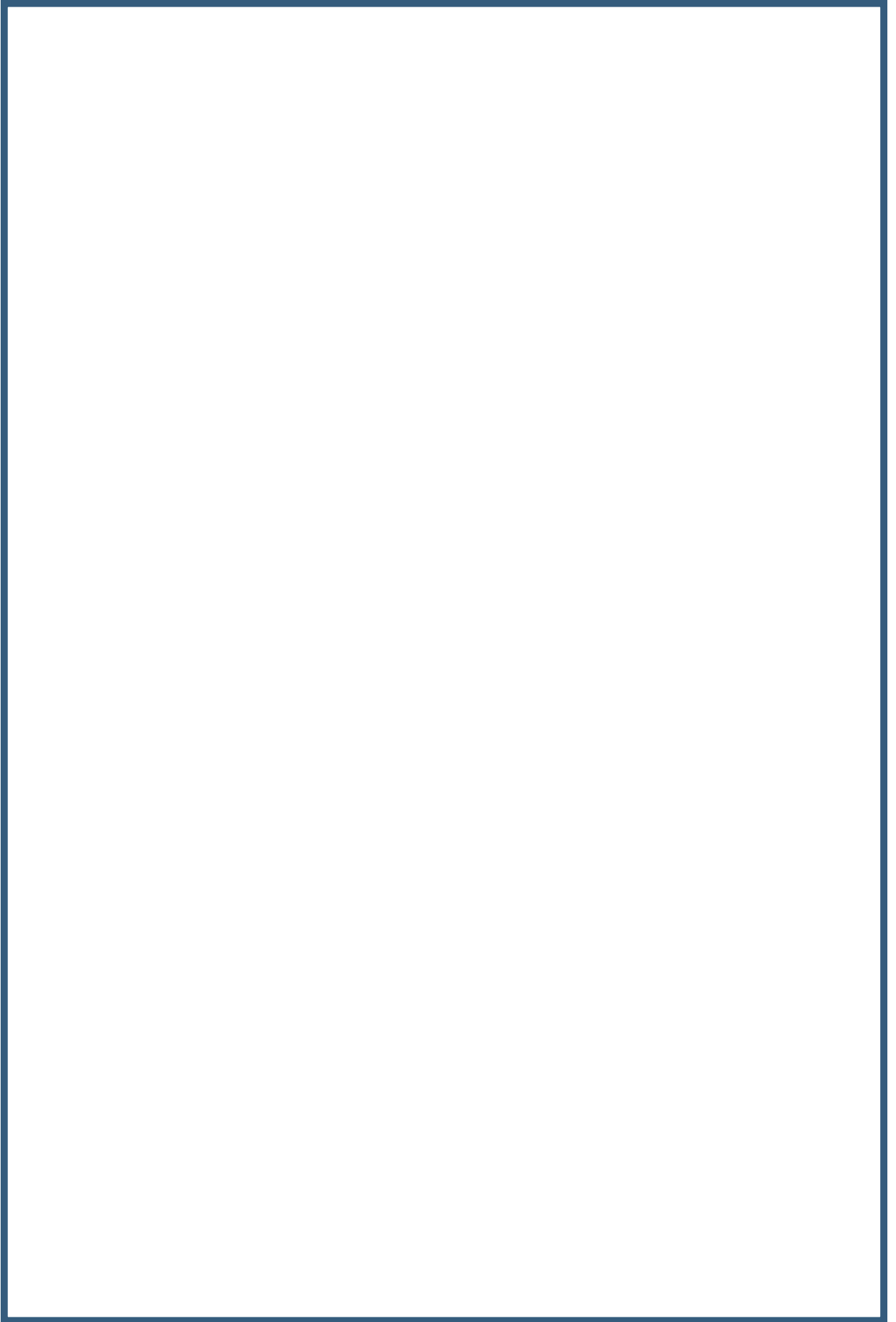
ALL: .foobar.edu EXCEPT terminalserver.foobar.edu

#

If you're going to protect the portmapper use the name "rpcbind" for the

daemon name. See rpcbind(8) and rpc.mountd(8) for further information.

#



3.3.3

Ensure /etc/hosts.deny is configured

Not Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message /etc/hosts.deny not configured

Time Taken 0.017261505126953125 seconds

Explanation:

/etc/hosts.deny: list of hosts that are _not_ allowed to access the system.

See the manual pages hosts_access(5) and hosts_options(5).

#

Example: ALL: some.host.name, .some.domain

**# ALL EXCEPT in.fingerd: other.host.name, .other.doma
in**

#

**# If you're going to protect the portmapper use the name "rpcbind
" for the**

**# daemon name. See rpcbind(8) and rpc.mountd(8) for further infor
mation.**

#

**# The PARANOID wildcard matches any host whose name does not matc
h its**

address.

#

You may wish to enable this to ensure any programs that don't

**# validate looked up hostnames still leave understandable logs. I
n past**

versions of Debian this has been the default.

ALL: PARANOID

3.3.4

Ensure permissions on /etc/hosts.allow are configured

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message /etc/hosts.allow permissions configured

Time Taken 0.02420806884765625 seconds

Explanation:

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

Access: 2021-08-02 15:11:09.014703300 +1000

3.3.5

Ensure permissions on /etc/hosts.deny are configured

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message /etc/hosts.deny permissions configured

Time Taken 0.02958989143371582 seconds

Explanation:

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

Access: 2021-08-02 15:11:09.018703300 +1000

3.4.1

Ensure DCCP is disabled

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	dccp cannot be mounted
Time Taken	0.05029606819152832 seconds
Explanation:	
install /bin/true	

3.4.2

Ensure SFTP is disabled

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	sftp cannot be mounted
Time Taken	0.0580294132232666 seconds

Explanation:

```
install /bin/true
```

3.4.3

Ensure RDS is disabled

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	rds cannot be mounted
Time Taken	0.04023170471191406 seconds
Explanation:	
<code>install /bin/true</code>	

3.4.4

Ensure TIPC is disabled

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	tipc cannot be mounted
Time Taken	0.03860616683959961 seconds
Explanation:	
install /bin/true	

3.5.1.1

Ensure IPv6 default deny firewall policy

Scored
Level 1 Server
Level 1 Workstation

Result **FAIL**
Message IPv6 default no deny policy
Time Taken **1.049421787261963 seconds**

Explanation:

Chain INPUT (policy ACCEPT)

Chain FORWARD (policy ACCEPT)

Chain OUTPUT (policy ACCEPT)

Following uses ipv6

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earlyprintk=ttyS0
```

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earlyprintk=ttyS0
```

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro recovery nomodeset dis_ucode_ldr console=tty1 console=ttyS0 earlyprintk=ttyS0
```

3.5.1.2

Ensure IPv6 loopback traffic is configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message IPv6 input loopback no config

Time Taken **0.03978323936462402 seconds**

Explanation:

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source
------	-------	--------	------	-----	----	-----	--------

		destination					
--	--	-------------	--	--	--	--	--

Following uses ipv6

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earlyprintk=ttyS0
```

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earlyprintk=ttyS0
```

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro recovery nomodeset dis_ucode_ldr console=tty1 console=ttyS0 earlyprintk=ttyS0
```

3.5.1.3

Ensure IPv6 outbound and established connections are configured

Not Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message IPv6 Table contains no config

Time Taken **0.03218197822570801 seconds**

Explanation:

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source
destination							

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source
destination							

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source
destination							

Following uses ipv6

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10
```

d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earlyprintk=ttyS0

linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earlyprintk=ttyS0

linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro recovery nomodeset dis_ucode_ldr console=tty1 console=ttyS0 earlyprintk=ttyS0

3.5.1.4

Ensure IPv6 firewall rules exist for all open ports

Not Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message open ports no firewall rule

Time Taken 0.04315376281738281 seconds

Explanation:

Following open ports were found

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer
tcp	LISTEN	0	128	[::]:22	
	[::]:*				

IPv6 input table configuration

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source
		destination					

3.5.2.1

Ensure default deny firewall policy

Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	no default deny firewall
Time Taken	0.01658153533935547 seconds

Explanation:

Chain INPUT (policy ACCEPT)

Chain FORWARD (policy ACCEPT)

Chain OUTPUT (policy ACCEPT)

3.5.2.2

Ensure loopback traffic is configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message fw input loopback no config

Time Taken 0.014026641845703125 seconds

Explanation:

Chain INPUT (policy ACCEPT 5090 packets, 1552K bytes)

pkts	bytes	target	prot	opt	in	out	source
------	-------	--------	------	-----	----	-----	--------

destination

3.5.2.3

Ensure outbound and established connections are configured

Not Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message iptables contains no config

Time Taken 0.011723041534423828 seconds

Explanation:

Chain INPUT (policy ACCEPT 5090 packets, 1552K bytes)

pkts	bytes	target	prot	opt	in	out	source
destination							

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source
destination							

Chain OUTPUT (policy ACCEPT 5440 packets, 1067K bytes)

pkts	bytes	target	prot	opt	in	out	source
destination							

3.5.2.4

Ensure firewall rules exist for all open ports

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message open ports no firewall rule

Time Taken 0.03283071517944336 seconds

Explanation:

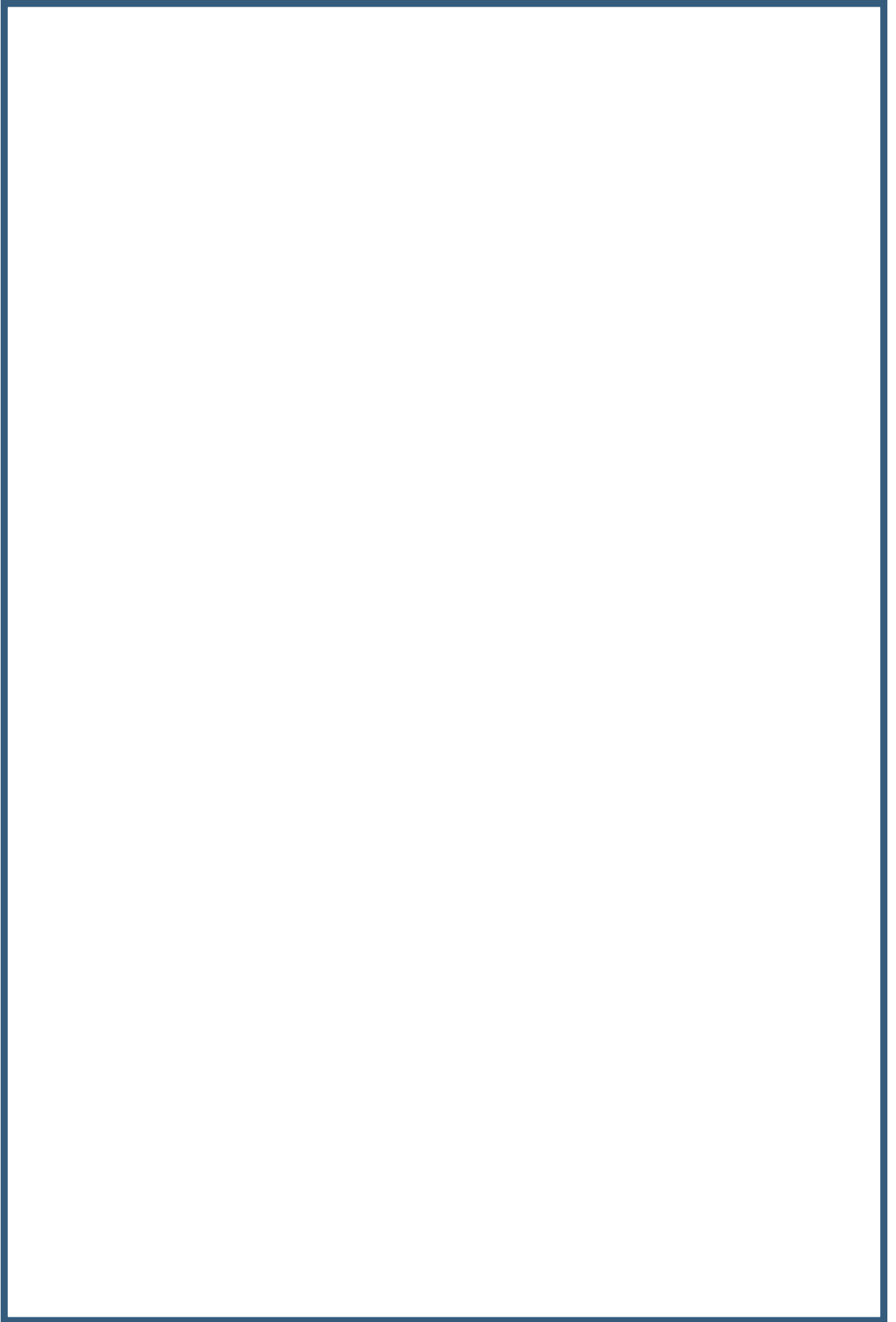
Following open ports were found

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer
Address:Port					
udp	UNCONN	0	0	127.0.0.53%lo:53	
0.0.0.0:*					
udp	UNCONN	0	0	10.3.0.4%eth0:68	
0.0.0.0:*					
tcp	LISTEN	0	128	127.0.0.53%lo:53	
0.0.0.0:*					
tcp	LISTEN	0	128	0.0.0.0:22	
0.0.0.0:*					

iptables input configuration

Chain INPUT (policy ACCEPT 5090 packets, 1552K bytes)

pkts	bytes	target	prot	opt	in	out	source
destination							



3.5.3

Ensure iptables is installed (distro specific)

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

iptables not checked (ind distro)

Time Taken

8.177757263183594e-05 seconds

Explanation:

Distribution was not specified

3.6

Ensure wireless interfaces are disabled

Not Scored

Level 1 Server

Level 2 Workstation

Result

PASS

Message

wireless interfaces disabled

Time Taken

0.012549638748168945 seconds

Explanation:

/bin/bash: iwconfig: command not found

3.7

Disable IPv6

Not Scored
Level 2 Server
Level 2 Workstation

Result FAIL

Message IPv6 enabled

Time Taken 0.02044987678527832 seconds

Explanation:

The following use IPv6

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earlyprintk=ttyS0
```

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earlyprintk=ttyS0
```

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro recovery nomodeset dis_ucode_ldr console=tty1 console=ttyS0 earlyprintk=ttyS0
```

4.1.1.1

Ensure audit log storage size is configured

Scored

Level 2 Server

Level 2 Workstation

Result PASS

Message audit log storage size is configured

Time Taken 0.016148805618286133 seconds

Explanation:

Ensure output is in compliance with site policy

max_log_file = 8

max_log_file_action = ROTATE

4.1.1.2

Ensure system is disabled when audit logs are full

Scored

Level 2 Server

Level 2 Workstation

Result PASS

Message system disabled when audit logs full

Time Taken 0.04952597618103027 seconds

Explanation:

action_mail_acct = root

admin_space_left_action = SUSPEND

4.1.1.3

Ensure audit logs are not automatically deleted

Scored

Level 2 Server

Level 2 Workstation

Result FAIL

Message audit logs automatically deleted

Time Taken 0.013926029205322266 seconds

Explanation:

max_log_file_action = ROTATE

4.1.2

Ensure auditd is installed (distro specific)

Scored

Level 2 Server

Level 2 Workstation

Result

CHEK

Message

auditd not checked (ind distro)

Time Taken

5.6743621826171875e-05 seconds

Explanation:

Distribution was not specified

4.1.3

Ensure auditd service is enabled

Scored
Level 2 Server
Level 2 Workstation

Result	FAIL
Message	auditd runlevel S02 not found
Time Taken	0.04308199882507324 seconds
Explanation:	
enabled	

ls /etc/rc*.d | grep auditd returned the following

K01auditd

K01auditd

S01auditd

S01auditd

S01auditd

S01auditd

K01auditd

4.1.4

Ensure auditing for processes that start prior to auditd is enabled (bootloader specific)

Scored

Level 2 Server

Level 2 Workstation

Result **FAIL**

Message processes prior to auditd not audited

Time Taken 0.01295018196105957 seconds

Explanation:

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earlyprintk=ttyS0
```

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earlyprintk=ttyS0
```

```
linux /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10d0-2ae6-4411-9086-8ccd221055fd ro recovery nomodeset dis_ucode_ldr console=tty1 console=ttyS0 earlyprintk=ttyS0
```

4.1.5

Ensure events that modify date and time information are collected

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

events modifying date and time not coll

Time Taken

0.031438350677490234 seconds

Explanation:

4.1.6

Ensure events that modify user/group information are collected

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

events modifying u/g info not coll

Time Taken

0.0374293327331543 seconds

Explanation:

4.1.7

Ensure events that modify the system's network environment are collected

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

events modifying system's n/w env not coll

Time Taken

0.0357968807220459 seconds

Explanation:

/bin/bash: grepsystem-locale: command not found

4.1.8

Ensure events that modify the system's Mandatory Access Controls are collected

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

events modifying system's MAC not coll

Time Taken

0.03191995620727539 seconds

Explanation:

4.1.9

Ensure login and logout events are collected

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

login and logout events not collected

Time Taken

0.029797792434692383 seconds

Explanation:

4.1.10

Ensure session initiation information is collected

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

session initiation info not collected

Time Taken

0.03132820129394531 seconds

Explanation:

4.1.11

Ensure discretionary access control permission modification events are collected

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

access control mod events not coll

Time Taken

0.03098607063293457 seconds

Explanation:

4.1.12

Ensure unsuccessful unauthorized file access attempts are collected

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

unauthorized file access not coll

Time Taken

0.03280186653137207 seconds

Explanation:

4.1.13

Ensure use of privileged commands is collected

Scored

Level 2 Server

Level 2 Workstation

Result **FAIL**

Message privileged commands not collected

Time Taken **0.07151317596435547 seconds**

Explanation:

Following partitions were found

/dev/sdb1 on / type ext4 (rw,relatime,discard)

/dev/sdb15 on /boot/efi type vfat (rw,relatime,fmask=0077,dmask=0077,codepage=437,iocharset=iso8859-1,shortname=mixed,errors=remount-ro)

/dev/sda1 on /mnt type ext4 (rw,relatime,x-systemd.requires=cloud-init.service)

ABOVE was found on /dev/sdb1

ABOVE was found on /dev/sdb15

ABOVE was found on /dev/sda1

4.1.14

Ensure successful file system mounts are collected

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

successful fs mounts not collected

Time Taken

0.034313201904296875 seconds

Explanation:

4.1.15

Ensure file deletion events by users are collected

Scored

Level 2 Server

Level 2 Workstation

Result FAIL

Message unlink, rename *.rules events not coll

Time Taken 0.03136897087097168 seconds

Explanation:

First rule - delete all

4.1.16

Ensure changes to system administration scope (sudoers) is collected

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

changes to sudoers not collected

Time Taken

0.030231714248657227 seconds

Explanation:

4.1.17

Ensure system administrator actions (sudolog) are collected

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

sudolog not collected

Time Taken

0.0317533016204834 seconds

Explanation:

4.1.18

Ensure kernel module loading and unloading is collected

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

kernel module not monitored

Time Taken

0.03107595443725586 seconds

Explanation:

4.1.19

Ensure the audit configuration is immutable

Scored

Level 2 Server

Level 2 Workstation

Result

FAIL

Message

audit configuration is mutable

Time Taken

0.01501154899597168 seconds

Explanation:

-f 1

4.2.1.1

Ensure rsyslog is installed (distro specific)

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

rsyslog not checked (ind distro)

Time Taken

6.818771362304688e-05 seconds

Explanation:

Distribution was not specified

4.2.1.2

Ensure rsyslog Service is enabled

Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	rsyslog runlevel S02 not found
Time Taken	0.049193382263183594 seconds
Explanation:	
enabled	

ls /etc/rc*.d | grep rsyslog returned the following

K01rsyslog

K01rsyslog

S01rsyslog

S01rsyslog

S01rsyslog

S01rsyslog

K01rsyslog

4.2.1.3

Ensure logging is configured

Not Scored
Level 1 Server
Level 1 Workstation

Result CHEK

Message logging is configured

Time Taken 0.05378460884094238 seconds

Explanation:

Review the contents of rsyslog.conf

```
# /etc/rsyslog.conf      Configuration file for rsyslog.

#

#           For more information see

#           /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html

#

# Default logging rules can be found in /etc/rsyslog.d/50-default.conf
```

#####

MODULES

#####

module(load="imuxsock") # provides support for local system logging

#module(load="immark") # provides --MARK-- message capability

provides UDP syslog reception

#module(load="imudp")

#input(type="imudp" port="514")

provides TCP syslog reception

#module(load="imtcp")

#input(type="imtcp" port="514")

provides kernel logging support and enable non-kernel klog messages

module(load="imklog" permitnonkernelfacility="on")

#####

GLOBAL DIRECTIVES

#####

#

Use traditional timestamp format.

To enable high precision timestamps, comment out the following line.

#

\$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

Filter duplicated messages

\$RepeatedMsgReduction on

#

Set the default permissions for all log files.

#

\$FileOwner syslog

\$FileGroup adm

\$FileCreateMode 0640

\$DirCreateMode 0755

\$Umask 0022

\$PrivDropToUser syslog

\$PrivDropToGroup syslog

#

Where to place spool and state files

#

\$WorkDirectory /var/spool/rsyslog

#

Include all config files in /etc/rsyslog.d/

#

\$IncludeConfig /etc/rsyslog.d/*.conf

Review the contents of rsyslog.d/*.conf

Log cloudinit generated log messages to file

:syslogtag, isequal, "[CLOUDINIT]" /var/log/cloud-init.log

comment out the following line to allow CLOUDINIT messages through.

Doing so means you'll also get CLOUDINIT messages in /var/log/syslog

& stop

Default rules for rsyslog.

#

For more information see **rsyslog.conf(5)** and **/etc**
/rsyslog.conf

#

First some standard log files. Log by facility.

#

auth,authpriv.* /var/log/auth.log

***.*;auth,authpriv.none -/var/log/syslog**

#cron.* /var/log/cron.log

#daemon.* -/var/log/daemon.log

kern.* -/var/log/kern.log

#lpr.* -/var/log/lpr.log

mail.* -/var/log/mail.log

#user.* -/var/log/user.log

#

Logging for the mail system. Split it up so that

it is easy to write scripts to parse these files.

#

#mail.info -/var/log/mail.info

#mail.warn -/var/log/mail.warn

mail.err /var/log/mail.err

#

Some "catch-all" log files.

#

##.=debug;

auth,authpriv.none;

news.none;mail.none -/var/log/debug

##.=info;*.=notice;*.=warn;

auth,authpriv.none;

cron,daemon.none;

mail,news.none -/var/log/messages

#

Emergencies are sent to everybody logged in.

#

.emerg :omusrmsg:

#

I like to have messages displayed on the console, but only on a virtual

console I usually leave idle.

#

#daemon,mail.*;

news.=crit;news.=err;news.=notice;

*.=debug;*.=info;

*.=notice;*.=warn /dev/tty8

verify that the log files are logging information

total 1076

-rw-r--r-- 1 root root 1545 Aug 2 15:15 alter natives.log

drwxr-xr-x 2 root root 4096 Sep 28 2018 appar mor

drwxr-xr-x 2 root root 4096 Aug 2 15:15 apt

drwxr-x--- 2 root adm 4096 Aug 2 15:15 audit

-rw-r----- 1 syslog adm 132387 Aug 2 15:49 auth.log

drwxr-xr-x 2 root root 4096 Aug 2 15:10 azure

-rw-rw---- 1 root utmp 53376 Aug 2 15:49 btmp

-rw-r-----	1	root	adm	9837	Aug	2	15:22	cloud
-init-output.log								
-rw-r--r--	1	syslog	adm	280009	Aug	2	15:22	cloud
-init.log								
drwxr-xr-x	2	root	root	4096	Apr	21	07:36	dist-
upgrade								
-rw-r--r--	1	root	root	103481	Aug	2	15:24	dpkg.
log								
drwxr-sr-x+	3	root	systemd-journal	4096	Aug	2	15:10	journ
al								
-rw-r-----	1	syslog	adm	112048	Aug	2	15:22	kern.
log								
drwxr-xr-x	2	landscape	landscape	4096	Aug	2	15:11	lands
cape								
-rw-rw-r--	1	root	utmp	292584	Aug	2	15:23	lastl
og								
drwxr-xr-x	2	root	root	4096	Nov	24	2018	lxd
drwxr-x---	2	root	adm	4096	Apr	14	22:52	samba
-rw-r-----	1	syslog	adm	285138	Aug	2	15:49	syslo
g								
-rw-----	1	root	root	64128	Aug	2	15:22	tally
log								
drwxr-x---	2	root	adm	4096	Aug	2	15:10	unatt
ended-upgrades								
-rw-r--r--	1	root	root	24433	Aug	2	15:37	waage
nt.log								

-rw-rw-r-- 1 root utmp 6144 Aug 2 15:23 wtmp

4.2.1.4

Ensure rsyslog default file permissions configured

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

rsyslog file permissions configured

Time Taken

0.015613079071044922 seconds

Explanation:

/etc/rsyslog.conf:\$FileCreateMode 0640

4.2.1.5

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

Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	rsyslog does not sends logs
Time Taken	0.017249345779418945 seconds
Explanation:	

4.2.1.6

Ensure remote rsyslog messages are only accepted on designated log hosts

Not Scored

Level 1 Server

Level 1 Workstation

Result

FAIL

Message

rsyslog messages not config

Time Taken

0.02888035774230957 seconds

Explanation:

4.2.2.1

Ensure journald is configured to send logs to rsyslog

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message journald does not send logs to rsyslog

Time Taken 0.0169830322265625 seconds

Explanation:

#ForwardToSyslog=yes

4.2.2.2

Ensure journald is configured to compress large log files

Scored

Level 1 Server

Level 1 Workstation

Result

FAIL

Message

journald not compress large log files

Time Taken

0.015765666961669922 seconds

Explanation:

#Compress=yes

4.2.2.3

Ensure journald is configured to write logfiles to persistent disk

Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	journald does not write logfiles
Time Taken	0.013826131820678711 seconds
Explanation:	
#Storage=auto	

4.2.3

Ensure permissions on all logfiles are configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message logfiles permissions not configured

Time Taken 0.021843671798706055 seconds

Explanation:

```
85991      4 -rw-r--r--    1 root    root      1545 Aug  2
15:15 /var/log/alternatives.log

85860     280 -rw-r-----    1 syslog  adm      285138 Aug  2
15:49 /var/log/syslog

63368     108 -rw-r--r--    1 root    root     103481 Aug  2
15:24 /var/log/dpkg.log

85864      24 -rw-r--r--    1 root    root     24433 Aug  2
15:37 /var/log/waagent.log

63357       8 -rw-rw-r--    1 root    utmp      6144 Aug  2
15:23 /var/log/wtmp

85863       4 -rw-r--r--    1 root    root      112 Aug  2
15:16 /var/log/unattended-upgrades/unattended-upgrades-shutdown.
log

274022    120 -rw-r-----    1 root    adm     117900 Aug  2
15:49 /var/log/audit/audit.log

86036    8192 -rw-r-----    1 root    systemd-journal 8388608
Aug  2 15:16 /var/log/journal/a68d3457c36440ec83d82e1f2ee7111f/u
ser-1000.journal
```


10253 8196 -rw-r----- 1 root systemd-journal 8388608
Aug 2 15:49 /var/log/journal/a68d3457c36440ec83d82e1f2ee7111f/s
ystem.journal

10684 8192 -rw-r----- 1 root systemd-journal 8388608
Aug 2 15:48 /var/log/journal/a68d3457c36440ec83d82e1f2ee7111f/u
ser-1001.journal

86037 0 -rw-r--r-- 1 root root 0
Aug 2 15:11 /var/log/landscape/sysinfo.log

63359 8 -rw-rw-r-- 1 root utmp 292584
Aug 2 15:23 /var/log/lastlog

10271 276 -rw-r--r-- 1 syslog adm 280009
Aug 2 15:22 /var/log/cloud-init.log

85862 136 -rw-r----- 1 syslog adm 132387
Aug 2 15:49 /var/log/auth.log

85861 112 -rw-r----- 1 syslog adm 112048
Aug 2 15:22 /var/log/kern.log

221 24 -rw-r--r-- 1 root root 24088
Aug 2 15:15 /var/log/apt/eipp.log.xz

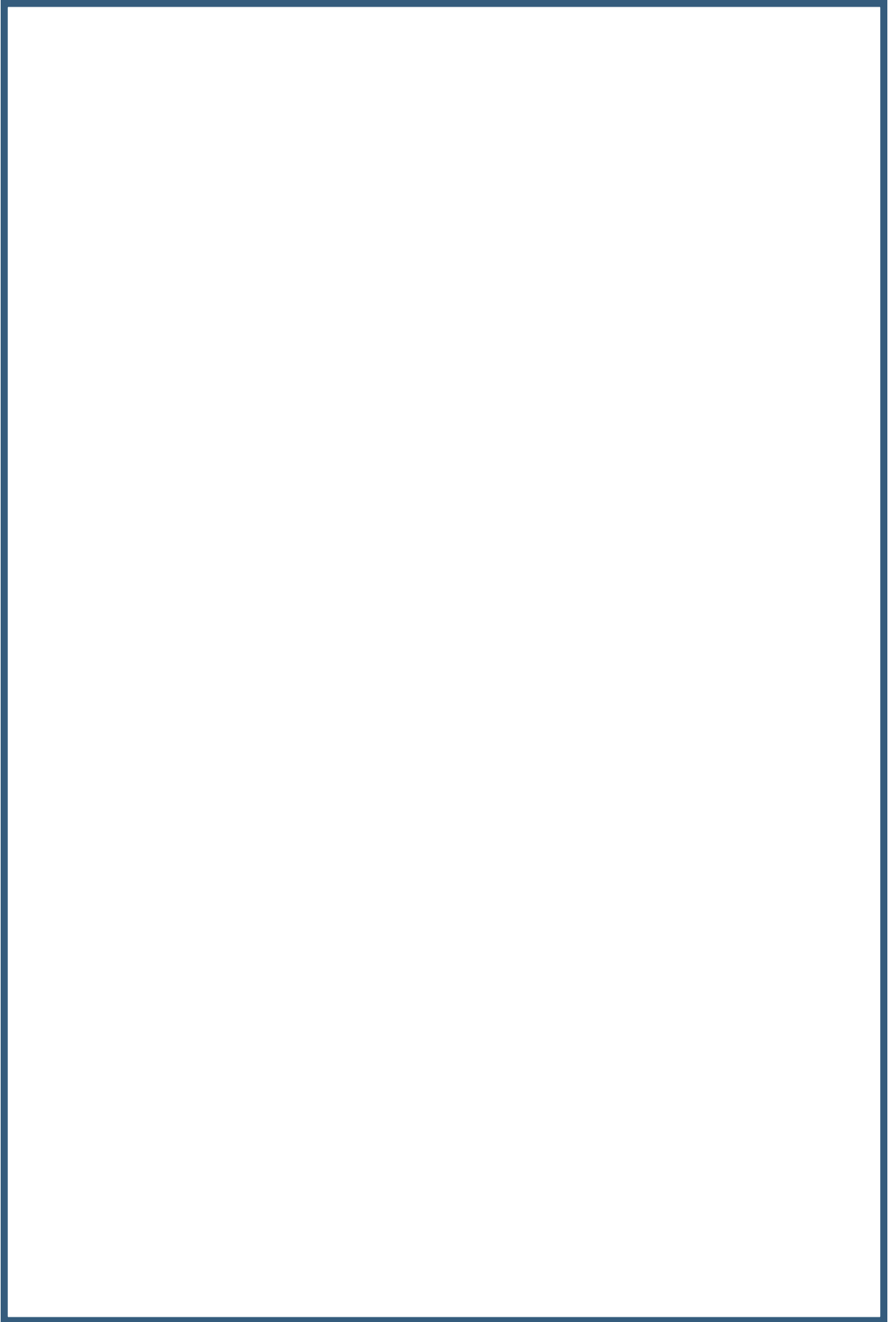
63362 12 -rw-r--r-- 1 root root 9951
Aug 2 15:15 /var/log/apt/history.log

63361 32 -rw-r----- 1 root adm 25171
Aug 2 15:15 /var/log/apt/term.log

310 8 -rw----- 1 root root 64128
Aug 2 15:22 /var/log/tallylog

10270 12 -rw-r----- 1 root adm 9837
Aug 2 15:22 /var/log/cloud-init-output.log

63358 60 -rw-rw---- 1 root utmp 53376
Aug 2 15:49 /var/log/btmp



4.3

Ensure logrotate is configured

Not Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

lograte is configured

Time Taken

0.027807235717773438 seconds

Explanation:

verify logs in logrotate.conf are rotated according to site policy

see "man logrotate" for details

rotate log files weekly

weekly

use the syslog group by default, since this is the owning group

of /var/log/syslog.

su root syslog

keep 4 weeks worth of backlogs

rotate 4

create new (empty) log files after rotating old ones

create

uncomment this if you want your log files compressed

#compress

packages drop log rotation information into this directory

include /etc/logrotate.d

no packages own wtmp, or btmp -- we'll rotate them here

/var/log/wtmp {

missingok

monthly

create 0664 root utmp

rotate 1

}

/var/log/btmp {

missingok

```
monthly

create 0660 root utmp

rotate 1

}
```

system-specific logs may be configured here

verify logs in logrotate directory are rotated according to site policy

```
/var/log/alternatives.log {
```

```
    monthly

    rotate 12

    compress

    delaycompress

    missingok

    notifempty

    create 644 root root

}
```

```
/var/log/apport.log {
```

```
    daily

    rotate 7
```

```
    delaycompress

    compress

    notifempty

    missingok
}
```

```
/var/log/apt/term.log {

    rotate 12

    monthly

    compress

    missingok

    notifempty
}
```

```
/var/log/apt/history.log {

    rotate 12

    monthly

    compress

    missingok

    notifempty
```

```
}
```

```
/var/log/dpkg.log {
```

```
monthly
```

```
rotate 12
```

```
compress
```

```
delaycompress
```

```
missingok
```

```
notifempty
```

```
create 644 root root
```

```
}
```

```
/var/log/lxd/lxd.log {
```

```
copytruncate
```

```
daily
```

```
rotate 7
```

```
delaycompress
```

```
compress
```

```
notifempty
```

```
missingok
```

```
}
```

/var/log/syslog

{

rotate 7

daily

missingok

notifempty

delaycompress

compress

postrotate

/usr/lib/rsyslog/rsyslog-rotate

endscript

}

/var/log/mail.info

/var/log/mail.warn

/var/log/mail.err

/var/log/mail.log

/var/log/daemon.log

/var/log/kern.log

/var/log/auth.log

/var/log/user.log

/var/log/lpr.log

/var/log/cron.log

/var/log/debug

/var/log/messages

{

rotate 4

weekly

missingok

notifempty

compress

delaycompress

sharedscripts

postrotate

/usr/lib/rsyslog/rsyslog-rotate

endscript

}

/var/log/ubuntu-advantage.log {

rotate 6

monthly

```
    compress

    delaycompress

    missingok

    notifempty
}

/var/log/unattended-upgrades/unattended-upgrades.log

/var/log/unattended-upgrades/unattended-upgrades-dpkg.log

/var/log/unattended-upgrades/unattended-upgrades-shutdown.log
{
    rotate 6

    monthly

    compress

    missingok

    notifempty
}

/var/log/waagent.log {

    compress

    monthly

    rotate 6

    notifempty
```

missingok

}

5.1.1

Ensure cron daemon is enabled

Scored
Level 1 Server
Level 1 Workstation

Result FAIL

Message cron daemon not found

Time Taken 0.026563167572021484 seconds

Explanation:

systemctl is-enabled crond returned the following

Failed to get unit file state for crond.service: No such file or directory

5.1.2

Ensure permissions on /etc/crontab are configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message perms on /etc/crontab not configured

Time Taken 0.01647496223449707 seconds

Explanation:

File: /etc/crontab

Size: 722 Blocks: 8 IO Block: 4096 regular file

Device: 811h/2065d Inode: 847 Links: 1

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

Access: 2021-08-02 15:15:01.500789919 +1000

Modify: 2021-08-02 15:14:47.124702445 +1000

Change: 2021-08-02 15:14:47.124702445 +1000

Birth: -

5.1.3

Ensure permissions on /etc/cron.hourly are configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message perms on /etc/cron.hourly not configured

Time Taken **0.015765666961669922 seconds**

Explanation:

File: /etc/cron.hourly

Size: 4096 Blocks: 8 IO Block: 4096 directory

Device: 811h/2065d Inode: 1338 Links: 2

Access: (0700/drwx-----) Uid: (0/ root) Gid: (0/ root)

Access: 2021-08-02 15:39:55.617748316 +1000

Modify: 2021-08-02 15:14:47.308703705 +1000

Change: 2021-08-02 15:14:47.308703705 +1000

Birth: -

5.1.4

Ensure permissions on /etc/cron.daily are configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message perms on /etc/cron.daily not configured

Time Taken **0.015924453735351562 seconds**

Explanation:

File: /etc/cron.daily

Size: 4096 Blocks: 8 IO Block: 4096 directory

Device: 811h/2065d Inode: 413 Links: 2

Access: (0700/drwx-----) Uid: (0/ root) Gid: (0/ root)

Access: 2021-08-02 15:39:55.561748166 +1000

Modify: 2021-08-02 15:14:47.456704719 +1000

Change: 2021-08-02 15:14:47.456704719 +1000

Birth: -

5.1.5

Ensure permissions on /etc/cron.weekly are configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message perms on /etc/cron.weekly not configured

Time Taken **0.015176057815551758 seconds**

Explanation:

File: /etc/cron.weekly

Size: 4096 Blocks: 8 IO Block: 4096 directory

Device: 811h/2065d Inode: 1342 Links: 2

Access: (0700/drwx-----) Uid: (0/ root) Gid: (0/ root)

Access: 2021-08-02 15:39:55.617748316 +1000

Modify: 2021-08-02 15:14:47.596705678 +1000

Change: 2021-08-02 15:14:47.596705678 +1000

Birth: -

5.1.6

Ensure permissions on /etc/cron.monthly are configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message perms on /etc/cron.monthly not configured

Time Taken 0.015791654586791992 seconds

Explanation:

File: /etc/cron.monthly

Size: 4096 Blocks: 8 IO Block: 4096 directory

Device: 811h/2065d Inode: 1340 Links: 2

Access: (0700/drwx-----) Uid: (0/ root) Gid: (0/ root)

Access: 2021-08-02 15:39:55.561748166 +1000

Modify: 2021-08-02 15:14:47.736706637 +1000

Change: 2021-08-02 15:14:47.736706637 +1000

Birth: -

5.1.7

Ensure permissions on /etc/cron.d are configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message perms on /etc/cron.d not configured

Time Taken 0.016788482666015625 seconds

Explanation:

File: /etc/cron.d

Size: 4096 Blocks: 8 IO Block: 4096 directory

Device: 811h/2065d Inode: 1334 Links: 2

Access: (0700/drwx-----) Uid: (0/ root) Gid: (0/ root)

Access: 2021-08-02 15:15:01.760791306 +1000

Modify: 2021-08-02 15:14:47.880707623 +1000

Change: 2021-08-02 15:14:47.880707623 +1000

Birth: -

5.1.8

Ensure at/cron is restricted to authorized users

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message /etc/at.deny exists

Time Taken 0.028311491012573242 seconds

Explanation:

stat: cannot stat '/etc/cron.deny': No such file or directory

stat /etc/at.deny returned the following

5.2.1

Ensure permissions on /etc/ssh/sshd_config are configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message perms on sshd_config not configured

Time Taken 0.020005464553833008 seconds

Explanation:

File: /etc/ssh/sshd_config

Size: 3435 Blocks: 8 IO Block: 4096 regular file

Device: 811h/2065d Inode: 273559 Links: 1

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

Access: 2021-08-02 15:15:29.664906871 +1000

Modify: 2021-08-02 15:14:11.488632143 +1000

Change: 2021-08-02 15:14:11.488632143 +1000

Birth: -

5.2.2

Ensure permissions on SSH private host key files are configured

Scored
Level 1 Server
Level 1 Workstation

Result **PASS**
Message SSH private host keys perms config
Time Taken **0.08729124069213867 seconds**

Explanation:

File: /etc/ssh/ssh_host_rsa_key

Size: 1823 Blocks: 8 IO Block: 4096 regular file

Device: 811h/2065d Inode: 309 Links: 1

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

Access: 2021-08-02 15:22:09.088727700 +1000

Modify: 2021-08-02 15:22:07.700727700 +1000

Change: 2021-08-02 15:22:07.700727700 +1000

Birth: -

File: /etc/ssh/ssh_host_dsa_key

Size: 1381 Blocks: 8 IO Block: 4096 regular file

Device: 811h/2065d Inode: 773 Links: 1

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

Access: 2021-08-02 15:22:07.800727700 +1000

Modify: 2021-08-02 15:22:07.800727700 +1000

Change: 2021-08-02 15:22:07.800727700 +1000

Birth: -

File: /etc/ssh/ssh_host_ed25519_key

Size: 399 Blocks: 8 IO Block: 4096 regular file

Device: 811h/2065d Inode: 922 Links: 1

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

Access: 2021-08-02 15:22:09.088727700 +1000

Modify: 2021-08-02 15:22:07.824727700 +1000

Change: 2021-08-02 15:22:07.824727700 +1000

Birth: -

File: /etc/ssh/ssh_host_ecdsa_key

Size: 505 Blocks: 8 IO Block: 4096 regular file

Device: 811h/2065d Inode: 917 Links: 1

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

Access: 2021-08-02 15:22:09.088727700 +1000

Modify: 2021-08-02 15:22:07.816727700 +1000

Change: 2021-08-02 15:22:07.816727700 +1000

Birth: -

5.2.3

Ensure permissions on SSH public host key files are configured

Scored
Level 1 Server
Level 1 Workstation

Result **PASS**

Message SSH public host keys perms config

Time Taken **0.09483027458190918 seconds**

Explanation:

File: /etc/ssh/ssh_host_ed25519_key.pub

Size: 94 Blocks: 8 IO Block: 4096 regular file

Device: 811h/2065d Inode: 2565 Links: 1

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

Access: 2021-08-02 15:22:07.840727700 +1000

Modify: 2021-08-02 15:22:07.824727700 +1000

Change: 2021-08-02 15:22:07.824727700 +1000

Birth: -

File: /etc/ssh/ssh_host_dsa_key.pub

Size: 602 Blocks: 8 IO Block: 4096 regular file

Device: 811h/2065d Inode: 915 Links: 1

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

Access: 2021-08-02 15:22:16.864727700 +1000

Modify: 2021-08-02 15:22:07.800727700 +1000

Change: 2021-08-02 15:22:07.800727700 +1000

Birth: -

File: /etc/ssh/ssh_host_rsa_key.pub

Size: 394 Blocks: 8 IO Block: 4096 regular file

Device: 811h/2065d Inode: 752 Links: 1

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

Access: 2021-08-02 15:22:07.840727700 +1000

Modify: 2021-08-02 15:22:07.700727700 +1000

Change: 2021-08-02 15:22:07.700727700 +1000

Birth: -

File: /etc/ssh/ssh_host_ecdsa_key.pub

Size: 174 Blocks: 8 IO Block: 4096 regular file

Device: 811h/2065d Inode: 920 Links: 1

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

Access: 2021-08-02 15:22:07.840727700 +1000

Modify: 2021-08-02 15:22:07.816727700 +1000

Change: 2021-08-02 15:22:07.816727700 +1000

Birth: -

5.2.4

Ensure SSH Protocol is set to 2

Scored
Level 1 Server
Level 1 Workstation

Result **FAIL**

Message SSH Protocol not 2

Time Taken 0.014052152633666992 seconds

Explanation:

grep ^Protocol /etc/ssh/sshd_config returned the following

5.2.5

Ensure SSH LogLevel is appropriate

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	SSH LogLevel is appropriate
Time Taken	0.01798534393310547 seconds
Explanation:	
loglevel	INFO

5.2.6

Ensure SSH X11 forwarding is disabled

Scored

Level 2 Server

Level 1 Workstation

Result **FAIL**

Message SSH X11 forwarding not disabled

Time Taken **0.02095961570739746 seconds**

Explanation:

sshd -T | grep x11forwarding returned the following

x11forwarding no

5.2.7

Ensure SSH MaxAuthTries is set to 4 or less

Scored

Level 1 Server

Level 1 Workstation

Result

FAIL

Message

SSH MaxAuthTries is more than 4

Time Taken

0.02073979377746582 seconds

Explanation:

maxauthtries 6

5.2.8

Ensure SSH IgnoreRhosts is enabled

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message SSH IgnoreRhosts is disabled

Time Taken 0.026666641235351562 seconds

Explanation:

sshd -T | grep ignorerhosts returned the following

ignorerhosts yes

5.2.9

Ensure SSH HostbasedAuthentication is disabled

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message SSH HBA is enabled

Time Taken 0.029701709747314453 seconds

Explanation:

sshd -T | grep hostbasedauthentication returned the following

hostbasedauthentication no

5.2.10

Ensure SSH root login is disabled

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message SSH root login is enabled

Time Taken 0.03402376174926758 seconds

Explanation:

sshd -T | grep permitrootlogin returned the following

permitrootlogin no

5.2.11

Ensure SSH PermitEmptyPasswords is disabled

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message SSH PermitEmptyPasswords is enabled

Time Taken 0.030661344528198242 seconds

Explanation:

sshd -T | grep permitemptypasswords returned the following

permitemptypasswords no

5.2.12

Ensure SSH PermitUserEnvironment is disabled

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message SSH PermitUserEnvironment is enabled

Time Taken 0.03085780143737793 seconds

Explanation:

sshd -T | grep permituserenvironment returned the following

permituserenvironment no

5.2.13

Ensure only strong Ciphers are used

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

SSH only strong Ciphers are used

Time Taken

0.029379844665527344 seconds

Explanation:

ciphers chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com

5.2.14

Ensure only strong MAC algorithms are used

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

SSH only strong MAC algorithms are used

Time Taken

0.03024888038635254 seconds

Explanation:

macs **hmac-sha2-256, hmac-sha2-512, hmac-sha1**

5.2.15

Ensure only strong Key Exchange algorithms are used

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

SSH only strong Key Exchange algorithms are used

Time Taken

0.026840925216674805 seconds

Explanation:

kexalgorithms curve25519-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1

5.2.16

Ensure SSH Idle Timeout Interval is configured

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message SSH ClientAliveInterval more than 300

Time Taken 0.02977728843688965 seconds

Explanation:

clientaliveinterval 600

5.2.17

Ensure SSH LoginGraceTime is set to one minute or less

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

SSH LoginGraceTime is 60

Time Taken

0.03050065040588379 seconds

Explanation:

loggingracetime 60

5.2.18

Ensure SSH access is limited

Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	SSH access is not limited
Time Taken	0.11745810508728027 seconds
Explanation:	

5.2.19

Ensure SSH warning banner is configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message SSH warning banner is not configured

Time Taken 0.032148122787475586 seconds

Explanation:

sshd -T | grep banner returned the following

banner /etc/issue.net

5.2.20

Ensure SSH PAM is enabled

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	SSH PAM is enabled
Time Taken	0.023871183395385742 seconds
Explanation:	
usepam	yes

5.2.21

Ensure SSH AllowTcpForwarding is disabled

Scored

Level 2 Server

Level 2 Workstation

Result **FAIL**

Message SSH AllowTcpForwarding is enabled

Time Taken 0.03231215476989746 seconds

Explanation:

sshd -T | grep -i allowtcpforwarding returned the following

allowtcpforwarding no

5.2.22

Ensure SSH MaxStartups is configured

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

SSH MaxStartups is configured

Time Taken

0.03363656997680664 seconds

Explanation:

verify that output of MaxStartups matches site policy

maxstartups 10:30:100

5.2.23

Ensure SSH MaxSessions is set to 4 or less

Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

SSH MaxSessions is set to 10

Time Taken

0.03076958656311035 seconds

Explanation:

verify that output of MaxSessions matches site policy

maxsessions 10

5.3.1

Ensure password creation requirements are configured

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message password creation req not found

Time Taken 0.08434581756591797 seconds

Explanation:

cat: /etc/pam.d/system-auth: No such file or directory

cat: /etc/pam.d/system-auth: No such file or directory

cat: /etc/security/pwquality.conf: No such file or directory

5.3.2

Ensure logout for failed password attempts is configured

Not Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

failed password logout configured

Time Taken

0.041379690170288086 seconds

Explanation:

Verify password lockouts are configured and `pam_faillock.so` lines should surround a `pam_unix.so`

```
#
```

```
# /etc/pam.d/common-auth - authentication settings common to all services
```

```
#
```

```
# This file is included from other service-specific PAM config files,
```

```
# and should contain a list of the authentication modules that define
```

```
# the central authentication scheme for use on the system
```

```
# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the
```

```
# traditional Unix authentication mechanisms.
```

```
#
```


As of pam 1.0.1-6, this file is managed by pam-auth-update by default.

To take advantage of this, it is recommended that you configure any

local modules either before or after the default block, and use

pam-auth-update to manage selection of other modules. See

pam-auth-update(8) for details.

here are the per-package modules (the "Primary" block)

auth [success=1 default=ignore] pam_unix.so nullok_secure

here's the fallback if no module succeeds

auth requisite pam_deny.so

prime the stack with a positive return value if there isn't one already;

this avoids us returning an error just because nothing sets a success code

since the modules above will each just jump around

auth required pam_permit.so

and here are more per-package modules (the "Additional" block)

auth optional pam_cap.so

end of pam-auth-update config

cat: /etc/pam.d/system-auth: No such file or directory

cat: /etc/pam.d/password-auth: No such file or directory

5.3.3

Ensure password reuse is limited

Not Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message password reuse not limited

Time Taken 0.03675651550292969 seconds

Explanation:

cat: /etc/pam.d/system-auth: No such file or directory

5.3.4

Ensure password hashing algorithm is SHA-512

Not Scored

Level 1 Server

Level 1 Workstation

Result

CHEK

Message

password hashing algorithm is SHA-512

Time Taken

0.050145864486694336 seconds

Explanation:

ensure the sha512 option is included in all results

The "sha512" option enables salted SHA512 passwords. Without this option,

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

```
cat: /etc/pam.d/system-auth: No such file or directory
```

```
cat: /etc/pam.d/password-auth: No such file or directory
```

5.4.1.1

Ensure password expiration is 365 days or less

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message password expiration not 365 days or less

Time Taken **0.01309061050415039 seconds**

Explanation:

PASS_MAX_DAYS Maximum number of days a password may be used.

PASS_MAX_DAYS **99999**

5.4.1.2

Ensure minimum days between password changes is 7 or more

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message password changes not 7 days or more

Time Taken 0.01324772834777832 seconds

Explanation:

PASS_MIN_DAYS Minimum number of days allowed between password changes.

PASS_MIN_DAYS 0

5.4.1.3

Ensure password expiration warning days is 7 or more

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message password change warning gt 7 days

Time Taken 0.03527188301086426 seconds

Explanation:

verify PASS_WARN_AGE conforms to site policy

PASS_WARN_AGE Number of days warning given before a password expires.

PASS_WARN_AGE 7

Users PASS_WARN_AGE

adminuser:7

5.4.1.4

Ensure inactive password lock is 30 days or less

Scored

Level 1 Server

Level 1 Workstation

Result

FAIL

Message

inactive password lock more than 30 days

Time Taken

0.02373480796813965 seconds

Explanation:

INACTIVE=-1

5.4.1.5

Ensure all users last password change date is in the past

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message last password change date in past

Time Taken **1.0949528217315674 seconds**

Explanation:

```
for usr in $(cut -d: -f1 /etc/shadow); do [[ $(chage --list $usr  
| grep '^Last password change' | cut -d: -f2) > $(date) ]] && ech  
o "$usr :$(chage --list $usr | grep '^Last password change' | cut  
-d: -f2)"; done
```

returned the following

5.4.2

Ensure system accounts are secured

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

system accounts are secured

Time Taken

1.2039384841918945 seconds

Explanation:

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

/etc/host.conf: line 7: bad command `nospoof on'

5.4.3

Ensure default group for the root account is GID 0

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message root account GID is 0

Time Taken 0.011538982391357422 seconds

Explanation:

grep "^root:" /etc/passwd | cut -f4 -d: returned

0

5.4.4

Ensure default user umask is 027 or more restrictive

Scored

Level 1 Server

Level 1 Workstation

Result

FAIL

Message

umask not found in bashrc

Time Taken

0.008828878402709961 seconds

Explanation:

grep: /etc/bashrc: No such file or directory

5.4.5

Ensure default user shell timeout is 900 seconds or less

Scored

Level 2 Server

Level 2 Workstation

Result **FAIL**

Message shell timeout not in bashrc

Time Taken 0.03971266746520996 seconds

Explanation:

grep "^TMOUT" /etc/bashrc returned the following

grep: /etc/bashrc: No such file or directory

5.5

Ensure root login is restricted to system console

Not Scored

Level 1 Server

Level 1 Workstation

Result	PASS
Message	root login is restricted to system
Time Taken	0.00931549072265625 seconds

Explanation:

check if following are valid terminals that may be logged in directly as root

/etc/securetty: list of terminals on which root is allowed to login.

See securetty(5) and login(1).

#

console

#

Local X displays (allows empty passwords with pam_unix's nullok_secure)

#:0

#:0.0

#:0.1

#:1

#:1.0

#:1.1

#:2

#:2.0

#:2.1

#:3

#:3.0

#:3.1

#:...

#

#

=====

#

TTYS sorted by major number according to Documentation/devices.txt

#

=====

#

Virtual consoles

#tty1

#tty2

#tty3

#tty4

#tty5

#tty6

#tty7

#tty8

#tty9

#tty10

#tty11

#tty12

#tty13

#tty14

#tty15

#tty16

#tty17

#tty18

#tty19

#tty20

#tty21

#tty22

#tty23

#tty24

#tty25

#tty26

#tty27

#tty28

#tty29

#tty30

#tty31

#tty32

#tty33

#tty34

#tty35

#tty36

#tty37

#tty38

#tty39

#tty40

#tty41

#tty42

#tty43

#tty44

#tty45

#tty46

#tty47

#tty48

#tty49

#tty50

#tty51

#tty52

#tty53

#tty54

#tty55

#tty56

#tty57

#tty58

#tty59

#tty60

#tty61

#tty62

#tty63

#

UART serial ports

#ttyS0

#ttyS1

#ttyS2

#ttyS3

#ttyS4

#ttyS5

#...ttyS191

#

Serial Mux devices (Linux/PA-RISC only)

#ttyB0

#ttyB1

#...

#

Chase serial card

#ttyH0

#ttyH1

#...

#

Cyclades serial cards

#ttyC0

#ttyC1

#...ttyC31

#

Digiboard serial cards

#ttyD0

#ttyD1

#...

#

Stallion serial cards

#ttyE0

#ttyE1

#...ttyE255

#

Specialix serial cards

#ttyX0

#ttyX1

#...

#

Control Rocketport serial cards

#ttyR0

#ttyR1

#...

#

SDL RISCom serial cards

#ttyL0

#ttyL1

#...

#

Hayes ESP serial card

#ttyP0

#ttyP1

#...

#

Computone IntelliPort II serial card

#ttyF0

#ttyF1

#...ttyF255

#

Specialix I08+ serial card

#ttyW0

#ttyW1

#...

#

Control VS-1000 serial controller

#ttyV0

#ttyV1

#...

#

ISI serial card

#ttyM0

#ttyM1

#...

#

Technology Concepts serial card

#ttyT0

#ttyT1

#...

#

Specialix RIO serial card

#ttySR0

#ttySR1

#...ttySR511

#

Chase Research AT/PCI-Fast serial card

#ttyCH0

#ttyCH1

#...ttyCH63

#

Moxa Intellio serial card

#ttyMX0

#ttyMX1

#...ttyMX127

#

SmartIO serial card

#ttySI0

#ttySI1

#...

#

USB dongles

#ttyUSB0

#ttyUSB1

#ttyUSB2

#...

#

LinkUp Systems L72xx UARTs

#ttyLU0

#ttyLU1

#ttyLU2

#ttyLU3

#

StrongARM builtin serial ports

#ttySA0

#ttySA1

#ttySA2

#

SCI serial port (SuperH) ports and SC26xx serial ports

#ttySC0

#ttySC1

#ttySC2

#ttySC3

#ttySC4

#ttySC5

#ttySC6

#ttySC7

#ttySC8

#ttySC9

#

ARM "AMBA" serial ports

#ttyAM0

#ttyAM1

#ttyAM2

#ttyAM3

#ttyAM4

#ttyAM5

#ttyAM6

#ttyAM7

#ttyAM8

#ttyAM9

#ttyAM10

#ttyAM11

#ttyAM12

#ttyAM13

#ttyAM14

#ttyAM15

#

Embedded ARM AMBA PL011 ports (e.g. emulated by QEMU)

#ttyAMA0

#ttyAMA1

#ttyAMA2

#ttyAMA3

#

DataBooster serial ports

#ttyDB0

#ttyDB1

#ttyDB2

#ttyDB3

#ttyDB4

#ttyDB5

#ttyDB6

#ttyDB7

#

SGI Altix console ports

#ttySG0

#

Motorola i.MX ports

#ttySMX0

#ttySMX1

#ttySMX2

#

Marvell MPSC ports

#ttyMM0

#ttyMM1

#

PPC CPM (SCC or SMC) ports

#ttyCPM0

#ttyCPM1

#ttyCPM2

#ttyCPM3

#ttyCPM4

#ttyCPM5

#

Altix serial cards

#ttyIOC0

#ttyIOC1

#...ttyIOC31

#

NEC VR4100 series SIU

#ttyVR0

#

NEC VR4100 series SSIU

#ttyVR1

#

Altix ioc4 serial cards

#ttyIOC84

#ttyIOC85

#...ttyIOC115

#

Altix ioc3 serial cards

#ttySIOC0

#ttySIOC1

#...ttySIOC31

#

PPC PSC ports

#ttyPSC0

#ttyPSC1

#ttyPSC2

#ttyPSC3

#ttyPSC4

#ttyPSC5

#

ATMEL serial ports

#ttyAT0

#ttyAT1

#...ttyAT15

#

Hilscher netX serial port

#ttyNX0

#ttyNX1

#...ttyNX15

#

Xilinx uartlite - port

#ttyUL0

#ttyUL1

#ttyUL2

#ttyUL3

#

Xen virtual console - port 0

#xvc0

#

pmac_zilog - port

#ttyPZ0

#ttyPZ1

#ttyPZ2

#ttyPZ3

#

TX39/49 serial port

#ttyTX0

#ttyTX1

#ttyTX2

#ttyTX3

#ttyTX4

#ttyTX5

#ttyTX6

#ttyTX7

#

SC26xx serial ports (see SCI serial ports (SuperH))

#

MAX3100 serial ports

#ttyMAX0

#ttyMAX1

#ttyMAX2

#ttyMAX3

#

OMAP serial ports

#tty00

#tty01

#tty02

#tty03

#

User space serial ports

#ttyU0

#ttyU1

#

A2232 serial card

#ttyY0

#ttyY1

#

IBM 3270 terminal Unix tty access

#3270/tty1

#3270/tty2

#...

#

IBM iSeries/pSeries virtual console

#hvc0

#hvc1

#...

#IBM pSeries console ports

#hvs0

#hvs1

#hvs2

#

Equinox SST multi-port serial boards

#ttyEQ0

#ttyEQ1

#...ttyEQ1027

#

=====

#

Not in Documentation/Devices.txt

#

=====

#

Embedded Freescale i.MX ports

#ttymxc0

#ttymxc1

#ttymxc2

#ttymxc3

#ttymxc4

#ttymxc5

#

LXC (Linux Containers)

#lxc/console

#lxc/tty1

#lxc/tty2

#lxc/tty3

#lxc/tty4

#

Serial Console for MIPS Swarm

#duart0

#duart1

#

s390 and s390x ports in LPAR mode

#ttysclp0

#

ODROID XU4 serial console

#ttySAC0

#ttySAC1

#ttySAC2

#ttySAC3

5.6

Ensure access to the su command is restricted

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message access to su command not restricted

Time Taken 0.009054183959960938 seconds

Explanation:

```
# auth      required  pam_wheel.so
```

```
# auth      sufficient pam_wheel.so trust
```

```
# auth      required  pam_wheel.so deny group=nosu
```

6.1.1

Audit system file permissions (distro specific)

Not Scored

Level 2 Server

Level 2 Workstation

Result

CHEK

Message

system file perms not checked (ind distro)

Time Taken

0.0001266002655029297 seconds

Explanation:

Distribution was not specified

6.1.2

Ensure permissions on /etc/passwd are configured

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

/etc/passwd permissions configured

Time Taken

0.02051711082458496 seconds

Explanation:

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

Access: 2021-08-02 15:22:07.500727700 +1000

6.1.3

Ensure permissions on /etc/shadow are configured

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message /etc/shadow permissions configured

Time Taken 0.02890610694885254 seconds

Explanation:

Access: (0640/-rw-r-----) Uid: (0/ root) Gid: (42/
shadow)

Access: 2021-08-02 15:22:13.944727700 +1000

6.1.4

Ensure permissions on /etc/group are configured

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message /etc/group permissions configured

Time Taken 0.03609323501586914 seconds

Explanation:

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

Access: 2021-08-02 15:22:07.524727700 +1000

6.1.5

Ensure permissions on /etc/gshadow are configured

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message /etc/gshadow permissions configured

Time Taken 0.018808603286743164 seconds

Explanation:

Access: (0640/-rw-r-----) Uid: (0/ root) Gid: (42/
shadow)

Access: 2021-08-02 15:22:07.456727700 +1000

6.1.6

Ensure permissions on /etc/passwd- are configured

Scored

Level 1 Server

Level 1 Workstation

Result FAIL

Message /etc/passwd- permits group and others

Time Taken 0.025437593460083008 seconds

Explanation:

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

Access: 2021-08-02 15:15:02.000000000 +1000

6.1.7

Ensure permissions on /etc/shadow- are configured

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message /etc/shadow- permissions configured

Time Taken 0.029802799224853516 seconds

Explanation:

Access: (0640/-rw-r-----) Uid: (0/ root) Gid: (42/
shadow)

Access: 2021-08-02 15:22:09.000000000 +1000

6.1.8

Ensure permissions on /etc/group- are configured

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message /etc/group- permissions configured

Time Taken 0.02323746681213379 seconds

Explanation:

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

Access: 2021-08-02 15:15:02.000000000 +1000

6.1.9

Ensure permissions on /etc/gshadow- are configured

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

/etc/gshadow- permissions configured

Time Taken

0.022724390029907227 seconds

Explanation:

Access: (0640/-rw-r-----) Uid: (0/ root) Gid: (42/
shadow)

Access: 2021-08-02 15:15:02.000000000 +1000

6.1.10

Ensure no world writable files exist

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message world writable files does not exist

Time Taken **2.0857574939727783 seconds**

Explanation:

running `df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{ }' find '{ }' -xdev -type f -perm -0002` confirms that all world writable directories have the sticky variable set

6.1.11

Ensure no unowned files or directories exist

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message no unowned files or directories exist

Time Taken 6.159199237823486 seconds

Explanation:

running `df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{ }' find '{ }' -xdev -nouser` confirms that no unowned files or directories exist

6.1.12

Ensure no ungrouped files or directories exist

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message no ungrouped files or directories exist

Time Taken 5.468044757843018 seconds

Explanation:

running `df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{ }' find '{ }' -xdev -nogroup` confirms that no ungrouped files or directories exist

6.1.13

Audit SUID executables

Not Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	SUID executables found
Time Taken	1.9531769752502441 seconds

Explanation:

The following SUID executables exist

/sbin/mount.cifs

/bin/mount

/bin/fusermount

/bin/umount

/bin/ping

/bin/su

/usr/bin/newgrp

/usr/bin/chsh

/usr/bin/chfn

/usr/bin/newgidmap

/usr/bin/sudo

/usr/bin/gpasswd

/usr/bin/pkexec

/usr/bin/at

/usr/bin/traceroute6.iputils

/usr/bin/newuidmap

/usr/bin/passwd

/usr/lib/dbus-1.0/dbus-daemon-launch-helper

/usr/lib/eject/dmccrypt-get-device

/usr/lib/openssh/ssh-keysign

/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic

/usr/lib/policykit-1/polkit-agent-helper-1

/usr/lib/snapd/snap-confine

/usr/libexec/ssh-keysign

6.1.14

Audit SGID executables

Not Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	SGID executables found
Time Taken	1.8853542804718018 seconds

Explanation:

The following SGID executables exist

/sbin/pam_extrausers_chkpwd

/sbin/unix_chkpwd

/usr/bin/crontab

/usr/bin/mlocate

/usr/bin/bsd-write

/usr/bin/at

/usr/bin/expiry

/usr/bin/chage

/usr/bin/wall

/usr/lib/x86_64-linux-gnu/utempter/utempter

6.2.1

Ensure password fields are not empty

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message password fields are not empty

Time Taken 0.020413875579833984 seconds

Explanation:

```
awk -F: '($2 == "" ) { print $1 " does not have a password "}' /etc/shadow returned the following
```

6.2.2

Ensure no legacy "+" entries exist in /etc/passwd

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message no legacy "+" entries exist in /etc/passwd

Time Taken 0.015990495681762695 seconds

Explanation:

grep '^\\+: ' /etc/passwd returned the following

6.2.3

Ensure no legacy "+" entries exist in /etc/shadow

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message no legacy "+" entries exist in /etc/shadow

Time Taken 0.06541800498962402 seconds

Explanation:

grep '^\\+: ' /etc/shadow returned the following

6.2.4

Ensure no legacy "+" entries exist in /etc/group

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message no legacy "+" entries exist in /etc/group

Time Taken 0.014271259307861328 seconds

Explanation:

grep '^\\+: ' /etc/group returned the following

6.2.5

Ensure root is the only UID 0 account

Scored
Level 1 Server
Level 1 Workstation

Result PASS

Message root is the only UID 0 account

Time Taken 0.0282595157623291 seconds

Explanation:

awk -F: '(\$3 == 0) { print \$1 }' /etc/passwd returned the following

root

6.2.6 Ensure root PATH Integrity

Scored
Level 1 Server
Level 1 Workstation

Result **FAIL**

Message writable dir in root's executable path

Time Taken 0.5434272289276123 seconds

Explanation:

The following writable directories were found in root's executable path

/snap/bin is not a directory

6.2.7

Ensure all users' home directories exist

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message all users' home directories exist

Time Taken 0.1174306869506836 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_7.sh returned the following

6.2.8

Ensure users' home directories permissions are 750 or more restrictive

Scored

Level 1 Server

Level 1 Workstation

Result **FAIL**

Message Group or world-writable home directories

Time Taken 0.3685739040374756 seconds

Explanation:

The following users have Group or world-writable home directories

Other Read permission set on the home directory (/home/packer) of user packer

Other Execute permission set on the home directory (/home/packer) of user packer

Other Read permission set on the home directory (/home/adminuser) of user adminuser

Other Execute permission set on the home directory (/home/adminuser) of user adminuser

6.2.9

Ensure users own their home directories

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

users own their home directories

Time Taken

0.13345885276794434 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_9.sh returned the following

6.2.10

Ensure users' dot files are not group or world writable

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message users' . files not group or world-writable

Time Taken 0.6089422702789307 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_10.sh returned the following

6.2.11

Ensure no users have .forward files

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message no users have .forward files

Time Taken 0.10355186462402344 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_11.sh returned the following

6.2.12

Ensure no users have .netrc files

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message no users have .netrc files

Time Taken 0.10338497161865234 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_12.sh returned the following

6.2.13

Ensure users' .netrc Files are not group or world accessible

Scored

Level 1 Server

Level 1 Workstation

Result **PASS**

Message users' .netrc not group or world accessible

Time Taken 0.1025245189666748 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_13.sh returned the following

6.2.14

Ensure no users have .rhosts files

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message no users have .rhosts files

Time Taken 0.09179997444152832 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_14.sh returned the following

6.2.15

Ensure all groups in /etc/passwd exist in /etc/group

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message all groups in passwd exist in group

Time Taken 0.2799966335296631 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_15.sh returned the following

6.2.16

Ensure no duplicate UIDs exist

Scored
Level 1 Server
Level 1 Workstation

Result PASS

Message no duplicate UIDs exist

Time Taken 0.10528326034545898 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_16.sh returned the following

6.2.17

Ensure no duplicate GIDs exist

Scored
Level 1 Server
Level 1 Workstation

Result PASS

Message no duplicate GIDs exist

Time Taken 0.1112968921661377 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_17.sh returned the following

6.2.18

Ensure no duplicate user names exist

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

no duplicate user names exist

Time Taken

0.11181879043579102 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_18.sh returned the following

6.2.19

Ensure no duplicate group names exist

Scored

Level 1 Server

Level 1 Workstation

Result PASS

Message no duplicate group names exist

Time Taken 0.10027575492858887 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_19.sh returned the following

6.2.20

Ensure shadow group is empty

Scored

Level 1 Server

Level 1 Workstation

Result

PASS

Message

users not assigned to shadow group

Time Taken

0.02000594139099121 seconds

Explanation:

grep ^shadow:[^:]*:[^:]*:[^:]+ /etc/group returned the following