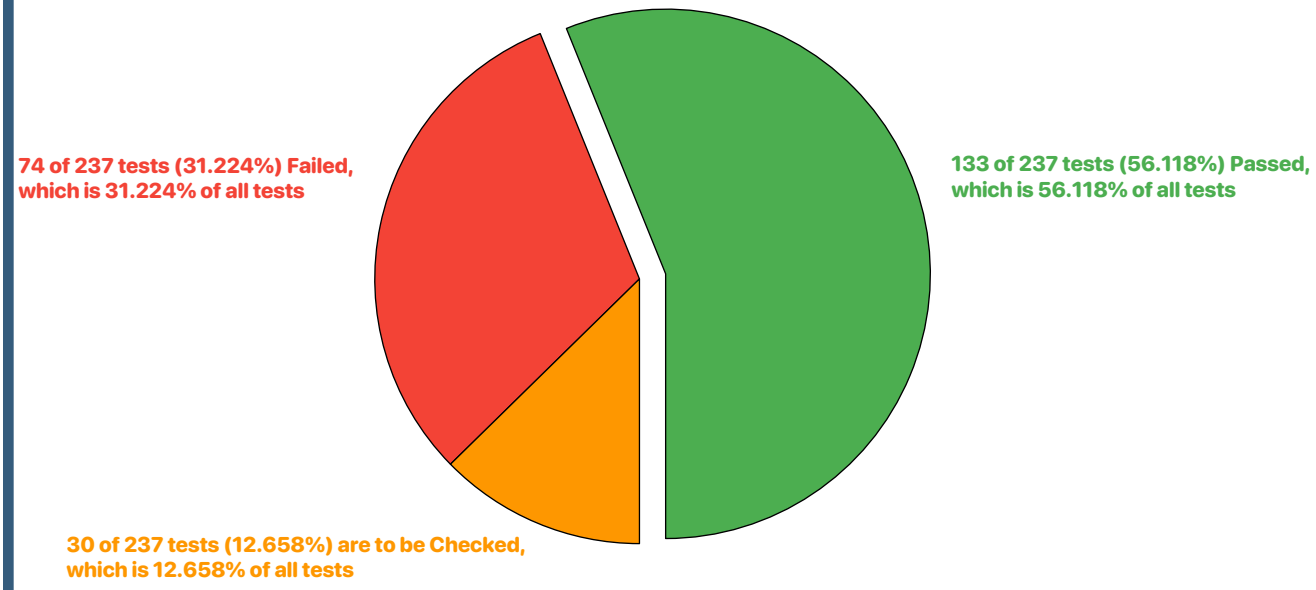
Result of CIS Distribution Independent Linux Benchmark v2.0.0

133 tests passed, where 128 were Scored.

This system's Score is 54%



Start Time (UTC): 2021-8-2 7:6:29

Start Time (Local): 2021-8-2 7:6:29

Finish Time (UTC): 2021-8-2 7:6:38

Finish Time (Local): 2021-8-2 7:6:38

Performed 237 tests in 8.811 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 cannot be mounted	PASS
1.1.1.8	vfat is mounted	CHEK
1.1.2	/tmp is configured	PASS
1.1.3	nodev is set on /tmp	PASS
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 set on /dev/shm	PASS
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 permissions configured	PASS
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	motd contains sensitive information	FAIL
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 permissions configured	PASS
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 is synchronized	PASS
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	dhcpd 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	broadcast ICMP requests ignored	PASS
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 router advert not accepted	PASS
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 not automatically deleted	PASS
4.1.2	autitd 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 coll	PASS
4.1.6	events modifying u/g info collected	PASS
4.1.7	network system-locale events not coll	FAIL

4.1.8	events modifying system's MAC coll	PASS
4.1.9	login and logout events are collected	PASS
4.1.10	session initiation info is collected	PASS
4.1.11	chmod *.rules events not coll	FAIL
4.1.12	EACCES *.rules events not coll	FAIL
4.1.13	privileged commands not collected	FAIL
4.1.14	mount *.rules events not coll	FAIL
4.1.15	unlink, rename *.rules events not coll	FAIL
4.1.16	changes to sudoers collected	PASS
4.1.17	sudolog collected	PASS
4.1.18	kernel module monitored	PASS
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 sends logs to rsyslog	PASS
4.2.2.2	jjournald compresses large log files	PASS
4.2.2.3	journald writes logfiles to persistent disk	PASS
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/cron.allow not configured	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 set to 2	PASS
5.2.5	SSH LogLevel is appropriate	PASS
5.2.6	SSH X11 forwarding not disabled	FAIL
5.2.7	SSH MaxAuthTries is set to 4	PASS
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 Idle Timeout Interval configured	PASS
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	PASS
5.2.23	SSH MaxSessions is set to 4	PASS
5.3.1	password creation req configured	CHEK
5.3.2	failed password lockout configured	CHEK
5.3.3	password reuse is limited	CHEK
5.3.4	password hashing algorithm is SHA-512	CHEK
5.4.1.1	users password expiration not found	FAIL
5.4.1.2	password changes not 7 days or more	FAIL
5.4.1.3	users password warn not found	FAIL
5.4.1.4	users password lock not found	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	root PATH Integrity maintained	PASS
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	0.05817055702209473 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	0.04479074478149414 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	0.044785499572753906 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	0.03151130676269531 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	0.059810161590576 17 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	0.04577350616455078 seconds

Explanation:

1.1.1.7
Ensure mounting of udf filesystems is disabled

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	udf cannot be mounted
Time Taken	0.06582164764404297 seconds

Explanation:

```
install /bin/true
```

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	0.0192661285400390 62 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	0.03764748573303223 seconds

Explanation:

```
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
```

1.1.3
Ensure nodev option set on /tmp partition

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	nodev is set on /tmp
Time Taken	0.07052206993103027 seconds

Explanation:

```
mount | grep -E '\s/tmp\s' | grep -v nodev did not return anythin
g
```

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	0.07199430465698242 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	0.06926393508911133 seconds

Explanation:

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

tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
```

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	0.03574728965759277 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	0.034615516662597656 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	0.03624773025512695 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	0.036297082901000 98 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	0.035639762878417 97 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	0.03477334976196289 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	0.037938594818115234 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	0.03359723091125488 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	0.030295848846435547 seconds

Explanation:

```
/home does not exist. nodev cannot be set on a partition that doe
s 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	0.072723388671875 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	0.0807793140411377 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	PASS
Message	noexec is set on /dev/shm
Time Taken	0.07240533828735352 seconds

Explanation:

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

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	0.0354924201965332 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	0.04069161415100098 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	0.03901052474975586 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	1.5514981746673584 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 st
icky variable set
```

1.1.22
Disable Automounting

Scored
Level 1 Server
Level 2 Workstation

Result	PASS
Message	automounting could not be checked
Time Taken	0.048970699310302734 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	0.057193756103515625 seconds

Explanation:

```
install /bin/true
```

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	7.128715515136719e-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	1.621246337890625e-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	1.1682510375976562e-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	0.03009343147277832 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	PASS
Message	bootloader permissions configured
Time Taken	0.02578592300415039 seconds

Explanation:

```
Access: (0400/-r--------)  Uid: (    0/    root)   Gid: (    0/
  root)

Access: 2021-08-02 06:56:46.458141236 +0000
```

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	0.046802997589111133 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	0.02179265022277832 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	0.022142410278320312 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	0.0649564266204834 seconds

Explanation:

```
Following are configured properly

fs.suid_dumpable = 0



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

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




Following are configured improperly

grep: /etc/security/limits.d/*: No such file or directory
```

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	3.8337953090667725 seconds

Explanation:

```
Jul 30 05:59:10 ubuntu kernel: NX (Execute Disable) protection: a
ctive

Aug 02 06:46:34 pkrvmaz2t4o6q0i kernel: NX (Execute Disable) prot
ection: 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	0.04143071174621582 seconds

Explanation:

```
Following are configured properly

kernel.randomize_va_space = 2



/etc/sysctl.conf:kernel.randomize_va_space=2

/etc/sysctl.d/99-sysctl.conf: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	4.935264587402344e-05 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	4.076957702636719e-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	0.019279241561889 65 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	0.033177852630615234 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	0.027806043624877 93 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	5.888938903808594e-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	1.4781951904296875e-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	0.053092002868652344 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	0.024755239486694336 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	0.44552040100097656 seconds

Explanation:

```
apparmor module is loaded.

16 profiles are loaded.

16 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/chronyd
```

```
   /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.

1 processes have profiles defined.

1 processes are in enforce mode.

   /usr/sbin/chronyd (1076)

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	FAIL
Message	motd contains sensitive information
Time Taken	0.044176578521728516 seconds

Explanation:

```
Following OS [or] patch level information were found in the messa
ge of the day

Authorized uses only. All activity may be monitored and reported.
```

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	0.048879384994506836 seconds

Explanation:

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

Authorized uses only. All activity may be monitored and reported.
```

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	0.05217695236206055 seconds

Explanation:

```
Following OS [or] patch level information were found in the remot
e login banner

Authorized uses only. All activity may be monitored and reported.
```

1.7.1.4
Ensure permissions on /etc/motd are configured

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	/etc/motd permissions configured
Time Taken	0.023122549057006836 seconds

Explanation:

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

Access: 2021-08-02 06:46:41.805881834 +0000
```

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	0.023580551147460938 seconds

Explanation:

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

Access: 2021-08-02 06:46:47.009887574 +0000
```

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	0.022267580032348633 seconds

Explanation:

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

Access: 2021-08-02 06:50:22.985257318 +0000
```

1.7.2
Ensure GDM login banner is configured

Scored
Level 1 Server
Level 1 Workstation

Result	CHEK
Message	GDM not found
Time Taken	0.020014047622680664 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	8.0108642578125e-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	0.019565582275390625 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	0.020814895629882812 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	0.020627260208129883 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	0.22838163375854492 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	0.020751476287841797 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	0.055779457092285156 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	0.037777662277221 68 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	0.018765449523925 78 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	0.0195310115814209 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	0.027276039123535156 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	5.936622619628906e-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	0.021993875503540004 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	0.018820285797119 14 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	PASS
Message	system clock is synchronized
Time Taken	0.19572830200195312 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
```

Check

```
                      Local time: Mon 2021-08-02 07:06:31 UTC
                  Universal time: Mon 2021-08-02 07:06:31 UTC
                        RTC time: Mon 2021-08-02 07:06:30
                       Time zone: Etc/UTC (UTC, +0000)
       System clock synchronized: no
systemd-timesyncd.service active: yes
```

RTC in local TZ: no

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	5.054473876953125e-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	0.03624892234802246 seconds

Explanation:

```
systemctl is-enabled avahi-daemon returned the following

Failed to get unit file state for avahi-daemon.service: No such f
ile 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	0.03089594841003418 seconds

Explanation:

```
systemctl is-enabled cups returned the following

Failed to get unit file state for cups.service: No such file or d
irectory
```

2.2.5
Ensure DHCP Server is not enabled

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	dhcpd not found
Time Taken	0.031173229217529297 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	0.05702853202819824 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	0.10870695114135742 seconds

Explanation:

```
systemctl is-enabled nfs returned the following

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



systemctl is-enabled rpcbind returned the following

Failed to get unit file state for rpcbind.service: No such file o
r 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	0.051450252532958984 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	0.03915095329284668 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	0.039166927337646484 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	0.03703570365905762 seconds

Explanation:

```
systemctl is-enabled dovecot returned the following

Failed to get unit file state for dovecot.service: No such file o
r directory
```

2.2.12
Ensure Samba is not enabled

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	smb not found
Time Taken	0.037038326263427734 seconds

Explanation:

```
systemctl is-enabled smb returned the following

Failed to get unit file state for smb.service: No such file or di
rectory
```

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	0.0384526252746582 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	0.03559541702270508 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	0.025522708892822266 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	0.035983085632324 22 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	0.035382747650146484 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	5.9366226196289 06e-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	1.5497207641601562e-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	1.5735626220703125e-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	1.1444091796875e-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	1.0967254638671875e-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	0.07462596893310547 seconds

Explanation:

```
net.ipv6.conf.all.forwarding = 0
```

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

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

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

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

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	0.07871413230895996 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	0.14774298667907715 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_rou
te = 0

/etc/sysctl.d/99-sysctl.conf:net.ipv6.conf.all.accept_source_rout
e=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	0.14989209175109863 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_redirec
ts=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	0.07331514358520508 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	0.07340335845947266 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	PASS
Message	broadcast ICMP requests ignored
Time Taken	0.035811424255371094 seconds

Explanation:

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

```
/etc/sysctl.conf:net.ipv4.icmp_echo_ignore_broadcasts=1
```

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

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	0.037100315093994 14 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	0.07232213020324707 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	0.03962135314941406 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	PASS
Message	IPv6 router advert not accepted
Time Taken	0.07385611534118652 seconds

Explanation:

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

```
/etc/sysctl.conf:net.ipv6.conf.default.accept_ra=0

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

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	9.083747863769531e-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	0.014391899108886719 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	0.01806163787841797 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	0.02343606948852539 seconds

Explanation:

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

Access: 2021-08-02 06:50:20.457250665 +0000
```

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	0.024363994598388672 seconds

Explanation:

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

Access: 2021-08-02 06:50:20.457250665 +0000
```

3.4.1
Ensure DCCP is disabled

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	dccp cannot be mounted
Time Taken	0.050797224044799805 seconds

Explanation:

```
install /bin/true
```

3.4.2
Ensure SCTP is disabled

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	sctp cannot be mounted
Time Taken	0.04835963249206543 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	0.039591073989868164 seconds

Explanation:

```
install /bin/true
```

3.4.4
Ensure TIPC is disabled

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	tipc cannot be mounted
Time Taken	0.0563809871673584 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	0.04514455795288086 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=f89a10
d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earl
yprintk=ttyS0

             linux     /boot/vmlinuz-5.4.0-1055-azure root=UUID=f
89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0
 earlyprintk=ttyS0

             linux     /boot/vmlinuz-5.4.0-1055-azure root=UUID=f
89a10d0-2ae6-4411-9086-8ccd221055fd ro recovery nomodeset dis_uco
de_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	0.04339194297790527 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=f89a10
d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earl
yprintk=ttyS0

             linux     /boot/vmlinuz-5.4.0-1055-azure root=UUID=f
89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0
 earlyprintk=ttyS0

             linux     /boot/vmlinuz-5.4.0-1055-azure root=UUID=f
89a10d0-2ae6-4411-9086-8ccd221055fd ro recovery nomodeset dis_uco
de_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	0.04161953926086426 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 1 packets, 56 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 earl
yprintk=ttyS0

            linux     /boot/vmlinuz-5.4.0-1055-azure root=UUID=f
89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0
 earlyprintk=ttyS0

            linux     /boot/vmlinuz-5.4.0-1055-azure root=UUID=f
89a10d0-2ae6-4411-9086-8ccd221055fd ro recovery nomodeset dis_uco
de_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 1.053661584854126 seconds

Explanation:

```
Following open ports were found

Netid  State    Recv-Q   Send-Q      Local Address:Port     Peer
Address:Port

udp    UNCONN   0        0                  [::1]:323
   [::]:*

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	0.022765636444091797 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	0.015145063400268555 seconds

Explanation:

```
Chain INPUT (policy ACCEPT 7166 packets, 36M 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	0.020059823989868164 seconds

Explanation:

```
Chain INPUT (policy ACCEPT 7166 packets, 36M 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 6989 packets, 1138K 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 0.03406071662902832 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           10.1.0.4%eth0:68
0.0.0.0:*

udp    UNCONN   0        0               127.0.0.1:323
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 7166 packets, 36M 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	4.76837158203125e-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	0.008275032043457031 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 0.020111083984375 seconds

Explanation:

The following use IPv6

```
        linux     /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10
d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earl
yprintk=ttyS0

             linux     /boot/vmlinuz-5.4.0-1055-azure root=UUID=f
89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0
 earlyprintk=ttyS0

             linux     /boot/vmlinuz-5.4.0-1055-azure root=UUID=f
89a10d0-2ae6-4411-9086-8ccd221055fd ro recovery nomodeset dis_uco
de_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	0.012875795364379883 seconds

Explanation:

```
Ensure output is in compliance with site policy

max_log_file = 10

max_log_file_action = keep_logs
```

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	0.04853415489196777 seconds

Explanation:

```
action_mail_acct = root
```

```
admin_space_left_action = halt
```

4.1.1.3
Ensure audit logs are not automatically deleted

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	audit logs not automatically deleted
Time Taken	0.017363786697387695 seconds

Explanation:

```
max_log_file_action = keep_logs
```

4.1.2
Ensure auditd is installed (distro specific)

Scored
Level 2 Server
Level 2 Workstation

Result	CHEK
Message	autitd not checked (ind distro)
Time Taken	7.009506225585938e-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	0.04666948318481445 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	0.01815938949584961 seconds

Explanation:

```
        linux     /boot/vmlinuz-5.4.0-1055-azure root=UUID=f89a10
d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0 earl
yprintk=ttyS0

             linux     /boot/vmlinuz-5.4.0-1055-azure root=UUID=f
89a10d0-2ae6-4411-9086-8ccd221055fd ro console=tty1 console=ttyS0
 earlyprintk=ttyS0

             linux     /boot/vmlinuz-5.4.0-1055-azure root=UUID=f
89a10d0-2ae6-4411-9086-8ccd221055fd ro recovery nomodeset dis_uco
de_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	PASS
Message	events modifying date and time coll
Time Taken	0.0429072380065918 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_3.rules:-a always,exit
-F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_3.rules:-a always,exit
-F arch=b32 -S clock_settime -k time-change

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_3.rules:-a always,exit
-F arch=b64 -S adjtimex -S settimeofday -k time-change

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_3.rules:-a always,exit
-F arch=b64 -S clock_settime -k time-change

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_3.rules:-w /etc/localti
me -p wa -k time-change

-a always,exit -F arch=b32 -S stime,settimeofday,adjtimex -F key=
time-change

-a always,exit -F arch=b32 -S clock_settime -F key=time-change

-a always,exit -F arch=b64 -S adjtimex,settimeofday -F key=time-c
hange

-a always,exit -F arch=b64 -S clock_settime -F key=time-change
```

```
-w /etc/localtime -p wa -k time-change
```

4.1.6

Ensure events that modify user/group information are collected

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	events modifying u/g info collected
Time Taken	0.03852057456970215 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_4.rules:-w /etc/group -
p wa -k identity

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_4.rules:-w /etc/passwd
-p wa -k identity

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_4.rules:-w /etc/gshadow
 -p wa -k identity

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_4.rules:-w /etc/shadow
-p wa -k identity

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_4.rules:-w /etc/securit
y/opasswd -p wa -k identity

-w /etc/group -p wa -k identity

-w /etc/passwd -p wa -k identity

-w /etc/gshadow -p wa -k identity

-w /etc/shadow -p wa -k identity

-w /etc/security/opasswd -p wa -k identity
```

4.1.7

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

Scored
Level 2 Server
Level 2 Workstation

Result	FAIL
Message	network system-locale events not coll
Time Taken	0.04456686973571777 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_5.rules:-a always,exit
-F arch=b64 -S sethostname -S setdomainname -k system-locale

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_5.rules:-a always,exit
-F arch=b32 -S sethostname -S setdomainname -k system-locale

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_5.rules:-w /etc/issue -
p wa -k system-locale

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_5.rules:-w /etc/issue.n
et -p wa -k system-locale

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_5.rules:-w /etc/hosts -
p wa -k system-locale

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_5.rules:-w /etc/network
 -p wa -k system-locale

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_5.rules:-w /etc/network
s -p wa -k system-locale
```

4.1.8

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

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	events modifying system's MAC coll
Time Taken	0.03944873809814453 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_6.rules:-w /etc/apparmor/ -p wa -k MAC-policy

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_6.rules:-w /etc/apparmor.d/ -p wa -k MAC-policy

-w /etc/apparmor -p wa -k MAC-policy

-w /etc/apparmor.d -p wa -k MAC-policy
```

4.1.9
Ensure login and logout events are collected

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	login and logout events are collected
Time Taken	0.038554906845092770 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_7.rules:-w /var/log/faillog -p wa -k logins

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_7.rules:-w /var/log/lastlog -p wa -k logins

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_7.rules:-w /var/log/tallylog -p wa -k logins

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_8.rules:-w /var/log/wtmp -p wa -k logins

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_8.rules:-w /var/log/btmp -p wa -k logins

-w /var/log/faillog -p wa -k logins

-w /var/log/lastlog -p wa -k logins

-w /var/log/tallylog -p wa -k logins

-w /var/log/wtmp -p wa -k logins

-w /var/log/btmp -p wa -k logins
```

4.1.10
Ensure session initiation information is collected

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	session initiation info is collected
Time Taken	0.03759145736694336 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_7.rules:-w /var/log/faillog -p wa -k logins

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_7.rules:-w /var/log/lastlog -p wa -k logins

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_7.rules:-w /var/log/tallylog -p wa -k logins

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_8.rules:-w /var/run/utmp -p wa -k session

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_8.rules:-w /var/log/wtmp -p wa -k logins

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_8.rules:-w /var/log/btmp -p wa -k logins

-w /var/log/faillog -p wa -k logins

-w /var/log/lastlog -p wa -k logins

-w /var/log/tallylog -p wa -k logins

-w /var/run/utmp -p wa -k session
```

```
-w /var/log/wtmp -p wa -k logins

-w /var/log/btmp -p wa -k logins
```

4.1.11

Ensure discretionary access control permission modification events are collected

Scored
Level 2 Server
Level 2 Workstation

Result	FAIL
Message	chmod *.rules events not coll
Time Taken	0.03782939910888672 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_9.rules:-a always,exit
-F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!
=4294967295 -k perm_mod

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_9.rules:-a always,exit
-F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=100
0 -F auid!=4294967295 -k perm_mod

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_9.rules:-a always,exit
-F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr
-S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295
 -k perm_mod

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_9.rules:-a always,exit
-F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!
=4294967295 -k perm_mod

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_9.rules:-a always,exit
-F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=100
0 -F auid!=4294967295 -k perm_mod

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_9.rules:-a always,exit
-F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr
-S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295
 -k perm_mod
```

```
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000
 -F auid!=-1 -F key=perm_mod

-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F aui
d>=1000 -F auid!=-1 -F key=perm_mod

-a always,exit -F arch=b32 -S setxattr,lsetxattr,fsetxattr,remove
xattr,lremovexattr,fremovexattr -F auid>=1000 -F auid!=-1 -F key=
perm_mod

-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000
 -F auid!=-1 -F key=perm_mod

-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F aui
d>=1000 -F auid!=-1 -F key=perm_mod

-a always,exit -F arch=b64 -S setxattr,lsetxattr,fsetxattr,remove
xattr,lremovexattr,fremovexattr -F auid>=1000 -F auid!=-1 -F key=
perm_mod
```

4.1.12

Ensure unsuccessful unauthorized file access attempts are collected

Scored
Level 2 Server
Level 2 Workstation

Result	FAIL
Message	EACCES *.rules events not coll
Time Taken	0.038173675537109375 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_10.rules:-a always,exit
 -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate
-F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_10.rules:-a always,exit
 -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate
-F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_10.rules:-a always,exit
 -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate
-F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_10.rules:-a always,exit
 -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate
-F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,opena
t -F exit=-EACCES -F auid>=1000 -F auid!=-1 -F key=access

-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,opena
t -F exit=-EPERM -F auid>=1000 -F auid!=-1 -F key=access

-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,opena
t -F exit=-EACCES -F auid>=1000 -F auid!=-1 -F key=access
```

```
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,opena
t -F exit=-EPERM -F auid>=1000 -F auid!=-1 -F key=access
```

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	0.07619762420654297 seconds

Explanation:

```
Following partitions were found

/dev/sda1 on / type ext4 (rw,relatime,discard)

/dev/sda15 on /boot/efi type vfat (rw,relatime,fmask=0077,dmask=0
077,codepage=437,iocharset=iso8859-1,shortname=mixed,errors=remou
nt-ro)

/dev/sdb1 on /mnt type ext4 (rw,relatime,x-systemd.requires=cloud
-init.service)



ABOVE was found on /dev/sda1



ABOVE was found on /dev/sda15



ABOVE was found on /dev/sdb1
```

4.1.14
Ensure successful file system mounts are collected

Scored
Level 2 Server
Level 2 Workstation

Result	FAIL
Message	mount *.rules events not coll
Time Taken	0.04561305046081543 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_12.rules:-a always,exit
 -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts


/etc/audit/rules.d/ubuntu1804cis_rule_4_1_12.rules:-a always,exit
 -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts


-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -F
key=mounts

-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=-1 -F
key=mounts
```

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	0.044920921325683594 seconds

Explanation:

```
/etc/audit/rules.d/audit.rules:## First rule - delete all

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_13.rules:-a always,exit
 -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>
=1000 -F auid!=4294967295 -k delete

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_13.rules:-a always,exit
 -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>
=1000 -F auid!=4294967295 -k delete

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_16.rules:-a always,exit
 -F arch=b64 -S init_module -S delete_module -k modules

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_16.rules:-a always,exit
 -F arch=b32 -S init_module -S delete_module -k modules

-a always,exit -F arch=b32 -S unlink,rename,unlinkat,renameat -F
auid>=1000 -F auid!=-1 -F key=delete

-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F
auid>=1000 -F auid!=-1 -F key=delete

-a always,exit -F arch=b64 -S init_module,delete_module -F key=mo
dules
```

```
-a always,exit -F arch=b32 -S init_module,delete_module -F key=mo
dules
```

4.1.16

Ensure changes to system administration scope (sudoers) is collected

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	changes to sudoers collected
Time Taken	0.04150795936584473 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_14.rules:-w /etc/sudoers -p wa -k scope

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_14.rules:-w /etc/sudoers.d/ -p wa -k scope

-w /etc/sudoers -p wa -k scope

-w /etc/sudoers.d -p wa -k scope
```

4.1.17
Ensure system administrator actions (sudolog) are collected

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	sudolog collected
Time Taken	0.0455014705657959 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_15.rules:-w /var/log/sudo.log -p wa -k actions

-w /var/log/sudo.log -p wa -k actions
```

4.1.18
Ensure kernel module loading and unloading is collected

Scored
Level 2 Server
Level 2 Workstation

Result	PASS
Message	kernel module monitored
Time Taken	0.033152103424072266 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_16.rules:-w /sbin/insmo
d -p x -k modules

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_16.rules:-w /sbin/rmmod
 -p x -k modules

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_16.rules:-w /sbin/modpr
obe -p x -k modules

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_16.rules:-a always,exit
 -F arch=b64 -S init_module -S delete_module -k modules

/etc/audit/rules.d/ubuntu1804cis_rule_4_1_16.rules:-a always,exit
 -F arch=b32 -S init_module -S delete_module -k modules

-w /sbin/insmod -p x -k modules

-w /sbin/rmmod -p x -k modules

-w /sbin/modprobe -p x -k modules

-a always,exit -F arch=b64 -S init_module,delete_module -F key=mo
dules

-a always,exit -F arch=b32 -S init_module,delete_module -F key=mo
```

dules

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	0.014327764511108398 seconds

Explanation:

```
/etc/audit/rules.d/ubuntu1804cis_rule_4_1_9.rules:-a always,exit
-F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr
-S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295
 -k perm_mod
```

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	5.125999450683594e-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	0.047426700592041016 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	0.05114316940307617 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-defaul
t.conf




##################

#### MODULES ####
```

```
#################


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

#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 mess
ages

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 kernel generated UFW log messages to file

:msg,contains,"[UFW " /var/log/ufw.log



# Uncomment the following to stop logging anything that matches t
he last rule.

# Doing this will stop logging kernel generated UFW log messages
to the file

# normally containing kern.* messages (eg, /var/log/kern.log)

#& stop
```

```
# Log cloudinit generated log messages to file

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



# comment out the following line to allow CLOUDINIT messages thro
ugh.

# Doing so means you'll also get CLOUDINIT messages in /var/log/s
yslog

& 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 1148

drwxr-xr-x  2 root      root              4096 Feb  2  2018 aide
```

```
-rw-r-----  1 root      root             1088 Jul 30 06:09 alter
natives.log

drwxr-xr-x  2 root      root             4096 Sep 27  2018 appar
mor

drwxr-xr-x  2 root      root             4096 Jul 30 06:10 apt

drwxr-x---  2 root      adm              4096 Jul 30 06:10 audit


-rw-r-----  1 syslog    adm             37874 Aug  2 07:06 auth.
log

drwxr-xr-x  3 root      root             4096 Aug  2 06:55 azure


-rw-rw----  1 root      utmp             4224 Aug  2 06:54 btmp

drwxr-xr-x  2 _chrony   _chrony          4096 Aug  2 06:55 chron
y

-rw-r-----  1 root      adm             10345 Aug  2 06:46 cloud
-init-output.log

-rw-r-----  1 syslog    adm            304757 Aug  2 06:46 cloud
-init.log

drwxr-xr-x  2 root      root             4096 Apr 20 21:36 dist-
upgrade

-rw-r-----  1 root      root           107796 Jul 30 06:10 dpkg.
log

drwxr-sr-x+ 3 root      systemd-journal  4096 Jul 30 05:59 journ
al

-rw-r-----  1 syslog    adm            118265 Aug  2 06:47 kern.
log

drwxr-xr-x  2 landscape landscape        4096 Jul 30 06:00 lands
```

```
cape

-rw-rw-r--  1 root      utmp            292584 Aug  2 06:56 lastl
og

drwxr-xr-x  2 root      root              4096 Nov 23  2018 lxd

-rw-r-----  1 syslog    adm                143 Aug  2 06:46 mail.
log

drwxr-x---  2 root      adm               4096 Apr 14 12:52 samba


-rw-------  1 root      root              8917 Aug  2 07:06 sudo.
log

-rw-r-----  1 syslog    adm             428760 Aug  2 07:06 syslo
g

-rw-------  1 root      root             64128 Aug  2 06:55 tally
log

-rw-------  1 root      root              1328 Aug  2 06:56 ubunt
u-advantage.log

drwxr-x---  2 root      adm               4096 Jul 30 06:00 unatt
ended-upgrades

-rw-r-----  1 root      root             29677 Aug  2 07:01 waage
nt.log

-rw-rw-r--  1 root      utmp              6144 Aug  2 06:56 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	0.017084360122680664 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	0.019092321395874023 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	0.03477907180786133 seconds

Explanation:

4.2.2.1
Ensure journald is configured to send logs to rsyslog

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	journald sends logs to rsyslog
Time Taken	0.0175020694732666 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	PASS
Message	jjournald compresses large log files
Time Taken	0.015071868896484375 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	PASS
Message	journald writes logfiles to persistent disk
Time Taken	0.016146421432495117 seconds

Explanation:

`Storage=persistent`

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	0.024989843368530273 seconds

Explanation:

```
   272661      4 -rw-r--r--   1 root     root         1828 Aug  2
 06:55 /var/log/azure/Microsoft.OSTCExtensions.VMAccessForLinux/e
xtension.log

    85991      4 -rw-r-----   1 root     root         1088 Jul 30
 06:09 /var/log/alternatives.log

    85863    420 -rw-r-----   1 syslog   adm        428760 Aug  2
 07:06 /var/log/syslog

    63368    112 -rw-r-----   1 root     root       107796 Jul 30
 06:10 /var/log/dpkg.log

    85860     32 -rw-r-----   1 root     root        29677 Aug  2
 07:01 /var/log/waagent.log

    63357      8 -rw-rw-r--   1 root     utmp         6144 Aug  2
 06:56 /var/log/wtmp

    85974      4 -rw-r-----   1 root     root          112 Jul 30
 06:11 /var/log/unattended-upgrades/unattended-upgrades-shutdown.
log

   258075   6732 -rw-r-----   1 root     adm       6885694 Aug  2
 07:06 /var/log/audit/audit.log
```

```
  270472  10248 -r--r-----   1 root     adm      10485839 Jul 30
 06:10 /var/log/audit/audit.log.1

    1731      4 -rw-------   1 root     root         1328 Aug  2
 06:56 /var/log/ubuntu-advantage.log

   85985   8192 -rw-r-----   1 root     systemd-journal  8388608
 Jul 30 06:11 /var/log/journal/f04b4779d5e64db0bc6e49a92978e646/u
ser-1000.journal

     755  49156 -rw-r-----   1 root     systemd-journal 50331648
 Aug  2 07:06 /var/log/journal/f04b4779d5e64db0bc6e49a92978e646/s
ystem.journal

    1655   8192 -rw-r-----   1 root     systemd-journal  8388608
 Aug  2 07:02 /var/log/journal/f04b4779d5e64db0bc6e49a92978e646/u
ser-1001.journal

   10253  32772 -rw-r-----   1 root     systemd-journal 33554432
 Jul 30 06:10 /var/log/journal/f04b4779d5e64db0bc6e49a92978e646/s
ystem@911d25f6ee9d495995d64702d9406507-0000000000000001-0005c850e
b18ad44.journal

   86399      4 -rw-r-----   1 syslog   adm                143
 Aug  2 06:46 /var/log/mail.log

   86004      0 -rw-r-----   1 root     root                 0
 Jul 30 06:00 /var/log/landscape/sysinfo.log

     399     12 -rw-------   1 root     root              8917
 Aug  2 07:06 /var/log/sudo.log

   63359     12 -rw-rw-r--   1 root     utmp            292584
 Aug  2 06:56 /var/log/lastlog

   10271    304 -rw-r-----   1 syslog   adm             304757
 Aug  2 06:46 /var/log/cloud-init.log

   85862     44 -rw-r-----   1 syslog   adm              37874
 Aug  2 07:06 /var/log/auth.log
```

```
   85864    116 -rw-r-----   1 syslog   adm                118265
Aug  2 06:47 /var/log/kern.log

      93     24 -rw-r--r--   1 root     root                23272
Jul 30 06:10 /var/log/apt/eipp.log.xz

   63362     12 -rw-r--r--   1 root     root                10679
Jul 30 06:10 /var/log/apt/history.log

   63361     44 -rw-r-----   1 root     adm                 40480
Jul 30 06:10 /var/log/apt/term.log

     310      8 -rw-------   1 root     root                64128
Aug  2 06:55 /var/log/tallylog

   10270     12 -rw-r-----   1 root     adm                 10345
Aug  2 06:46 /var/log/cloud-init-output.log

   63358      8 -rw-rw----   1 root     utmp                 4224
Aug  2 06:54 /var/log/btmp

  272584      4 -rw-r--r--   1 _chrony  _chrony               924
Aug  2 07:04 /var/log/chrony/tracking.log

  272587      4 -rw-r--r--   1 _chrony  _chrony              3151
Aug  2 07:04 /var/log/chrony/measurements.log

  272586      4 -rw-r--r--   1 _chrony  _chrony              1755
Aug  2 07:04 /var/log/chrony/statistics.log
```

4.3
Ensure logrotate is configured

Not Scored
Level 1 Server
Level 1 Workstation

Result	CHEK
Message	lograte is configured
Time Taken	0.0285036563873291 seconds

Explanation:

```
verify logs in logrotate.conf are rotated according to site polic
y

# see "man logrotate" for details

# rotate log files weekly

daily



# 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
    daily
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
```

```
    daily

    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 {

     daily

     rotate 12

     compress

     delaycompress

     missingok

     notifempty

     create 644 root root

}

/var/log/apt/term.log {

  rotate 12

  daily
```

```
  compress
  missingok
  notifempty
}

/var/log/apt/history.log {
  rotate 12
  daily
  compress
  missingok
  notifempty
}

/var/log/chrony/*.log {
    missingok
    nocreate
    sharedscripts
    postrotate
        /usr/bin/chronyc cyclelogs > /dev/null 2>&1 || true
    endscript
```

```
}
/var/log/dpkg.log {
     daily
     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

     daily

     missingok

     notifempty

     compress

     delaycompress

     sharedscripts

     postrotate

          /usr/lib/rsyslog/rsyslog-rotate

     endscript

}

/var/log/ubuntu-advantage.log {

    rotate 6

    daily

    compress
```

```
    delaycompress
    missingok
    notifempty
}
/var/log/ufw.log
{
     rotate 4
     daily
     missingok
     notifempty
     compress
     delaycompress
     sharedscripts
     postrotate
          invoke-rc.d rsyslog rotate >/dev/null 2>&1 || true
     endscript
}
/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
  daily
  compress
  missingok
  notifempty
}
/var/log/waagent.log {
    compress
    daily
    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	0.024384498596191406 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	0.016593217849731445 seconds

Explanation:

```
  File: /etc/crontab

  Size: 838             Blocks: 8          IO Block: 4096   regula
r file

Device: 801h/2049d      Inode: 847         Links: 1

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

Access: 2021-08-02 06:46:41.689438304 +0000

Modify: 2021-07-30 06:09:00.128554190 +0000

Change: 2021-07-30 06:10:17.572819980 +0000

 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	0.018314361572265625 seconds

Explanation:

```
  File: /etc/cron.hourly

  Size: 4096            Blocks: 8          IO Block: 4096   direct
ory

Device: 801h/2049d      Inode: 1338        Links: 2

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

Access: 2021-08-02 06:56:46.502141321 +0000

Modify: 2021-07-21 00:34:42.546971504 +0000

Change: 2021-07-30 06:10:17.716836635 +0000

 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	0.017779827117919922 seconds

Explanation:

```
  File: /etc/cron.daily

  Size: 4096            Blocks: 8          IO Block: 4096   direct
ory

Device: 801h/2049d      Inode: 413         Links: 2

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

Access: 2021-08-02 06:56:46.486141290 +0000

Modify: 2021-07-30 06:10:47.708305131 +0000

Change: 2021-07-30 06:10:47.708305131 +0000

 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	0.017778873443603516 seconds

Explanation:

```
  File: /etc/cron.weekly

  Size: 4096            Blocks: 8          IO Block: 4096   direct
ory

Device: 801h/2049d      Inode: 1342        Links: 2

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

Access: 2021-08-02 06:56:46.502141321 +0000

Modify: 2021-07-21 00:36:34.801522842 +0000

Change: 2021-07-30 06:10:18.004869946 +0000

 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	0.017221450805664062 seconds

Explanation:

```
  File: /etc/cron.monthly

  Size: 4096            Blocks: 8          IO Block: 4096   direct
ory

Device: 801h/2049d      Inode: 1340        Links: 2

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

Access: 2021-08-02 06:56:46.486141290 +0000

Modify: 2021-07-21 00:34:42.546971504 +0000

Change: 2021-07-30 06:10:18.148886602 +0000

 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	0.01866459846496582 seconds

Explanation:

```
  File: /etc/cron.d

  Size: 4096            Blocks: 8          IO Block: 4096   direct
ory

Device: 801h/2049d      Inode: 1334        Links: 2

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

Access: 2021-08-02 06:46:41.689438304 +0000

Modify: 2021-07-21 00:36:10.733835490 +0000

Change: 2021-07-30 06:10:18.296903720 +0000

 Birth: -
```

5.1.8
Ensure at/cron is restricted to authorized users

Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	/etc/cron.allow not configured
Time Taken	0.045999765396118164 seconds

Explanation:

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

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



stat /etc/at.allow returned the following

  File: /etc/cron.allow

  Size: 1               Blocks: 8          IO Block: 4096   regula
r file

Device: 801h/2049d      Inode: 272538      Links: 1

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

Access: 2021-07-30 06:10:19.068993011 +0000

Modify: 2021-07-30 06:10:18.976982370 +0000

Change: 2021-07-30 06:10:19.068993011 +0000
```

Birth: –

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	0.020214796066284 18 seconds

Explanation:

```
  File: /etc/ssh/sshd_config

  Size: 4119            Blocks: 16         IO Block: 4096   regula
r file

Device: 801h/2049d      Inode: 272535      Links: 1

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

Access: 2021-08-02 06:46:41.805881834 +0000

Modify: 2021-07-30 06:10:23.441498689 +0000

Change: 2021-07-30 06:10:23.441498689 +0000

 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 0.10645604133605957 seconds

Explanation:

```
  File: /etc/ssh/ssh_host_rsa_key

  Size: 1675            Blocks: 8          IO Block: 4096   regula
r file

Device: 801h/2049d      Inode: 221         Links: 1

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

Access: 2021-08-02 06:46:41.813881843 +0000

Modify: 2021-08-02 06:46:41.193480196 +0000

Change: 2021-08-02 06:46:41.193480196 +0000

 Birth: -

  File: /etc/ssh/ssh_host_dsa_key

  Size: 668             Blocks: 8          IO Block: 4096   regula
r file

Device: 801h/2049d      Inode: 288         Links: 1
```

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

Access: 2021-08-02 06:46:41.213478507 +0000

Modify: 2021-08-02 06:46:41.213478507 +0000

Change: 2021-08-02 06:46:41.213478507 +0000

 Birth: -

  File: /etc/ssh/ssh_host_ed25519_key

  Size: 411           Blocks: 8          IO Block: 4096   regula
r file

Device: 801h/2049d     Inode: 429         Links: 1

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

Access: 2021-08-02 06:46:41.813881843 +0000

Modify: 2021-08-02 06:46:41.229477155 +0000

Change: 2021-08-02 06:46:41.229477155 +0000

 Birth: -

  File: /etc/ssh/ssh_host_ecdsa_key

  Size: 227           Blocks: 8          IO Block: 4096   regula
r file

Device: 801h/2049d     Inode: 427         Links: 1

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

Access: 2021-08-02 06:46:41.813881843 +0000
```

```
Modify: 2021-08-02 06:46:41.225477493 +0000

Change: 2021-08-02 06:46:41.225477493 +0000

 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	0.11201190948486328 seconds

Explanation:

```
  File: /etc/ssh/ssh_host_ed25519_key.pub

  Size: 99              Blocks: 8          IO Block: 4096   regula
r file

Device: 801h/2049d      Inode: 432         Links: 1

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

Access: 2021-08-02 06:46:41.813881843 +0000

Modify: 2021-08-02 06:46:41.229477155 +0000

Change: 2021-08-02 06:46:41.229477155 +0000

 Birth: -

  File: /etc/ssh/ssh_host_dsa_key.pub

  Size: 607             Blocks: 8          IO Block: 4096   regula
r file

Device: 801h/2049d      Inode: 400         Links: 1
```

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

Access: 2021-08-02 06:46:46.973887534 +0000

Modify: 2021-08-02 06:46:41.213478507 +0000

Change: 2021-08-02 06:46:41.213478507 +0000

 Birth: -

  File: /etc/ssh/ssh_host_rsa_key.pub

  Size: 399           Blocks: 8          IO Block: 4096   regula
r file

Device: 801h/2049d     Inode: 236         Links: 1

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

Access: 2021-08-02 06:46:41.229477155 +0000

Modify: 2021-08-02 06:46:41.193480196 +0000

Change: 2021-08-02 06:46:41.193480196 +0000

 Birth: -

  File: /etc/ssh/ssh_host_ecdsa_key.pub

  Size: 179           Blocks: 8          IO Block: 4096   regula
r file

Device: 801h/2049d     Inode: 428         Links: 1

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

Access: 2021-08-02 06:46:41.229477155 +0000
```

```
Modify: 2021-08-02 06:46:41.225477493 +0000

Change: 2021-08-02 06:46:41.225477493 +0000

 Birth: -
```

5.2.4
Ensure SSH Protocol is set to 2

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	SSH Protocol set to 2
Time Taken	0.013033628463745117 seconds

Explanation:

```
Protocol 2
```

5.2.5
Ensure SSH LogLevel is appropriate

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	SSH LogLevel is appropriate
Time Taken	0.033574581146240234 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	0.032755374908447266 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	PASS
Message	SSH MaxAuthTries is set to 4
Time Taken	0.04264330863952637 seconds

Explanation:

```
maxauthtries 4
```

5.2.8
Ensure SSH IgnoreRhosts is enabled

Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	SSH IgnoreRhosts is disabled
Time Taken	0.037818908691406 25 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	0.038366794586181 64 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	0.039214134216308594 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	0.03486180305480957 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	0.03578996658325195 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	0.03627419471740723 seconds

Explanation:

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

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	0.03617429733276367 seconds

Explanation:

```
macs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,
umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@ope
nssh.com
```

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	0.04043173789978027 seconds

Explanation:

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

5.2.16
Ensure SSH Idle Timeout Interval is configured

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	SSH Idle Timeout Interval configured
Time Taken	0.07694888114929199 seconds

Explanation:

```
clientaliveinterval 300
```

```
clientalivecountmax 3
```

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	0.039173841476440 43 seconds

Explanation:

```
logingracetime 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	0.1396467685699463 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	0.0373225212097168 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	0.03749704360961914 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	0.038910627365112305 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	PASS
Message	SSH MaxStartups is configured
Time Taken	0.038129568099975586 seconds

Explanation:

```
maxstartups 10:30:60
```

5.2.23
Ensure SSH MaxSessions is set to 4 or less

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	SSH MaxSessions is set to 4
Time Taken	0.0392301082611084 seconds

Explanation:

```
maxsessions 4
```

5.3.1
Ensure password creation requirements are configured

Scored
Level 1 Server
Level 1 Workstation

Result	CHEK
Message	password creation req configured
Time Taken	0.08700251579284668 seconds

Explanation:

```
Verify password creation requirements conform to organization pol
icy and minlen is 14 or more

# Configuration for systemwide password quality limits

# Defaults:

#

# Number of characters in the new password that must not be prese
nt in the

# old password.

# difok = 1

#

# Minimum acceptable size for the new password (plus one if

# credits are not disabled which is the default). (See pam_crackl
ib manual.)

# Cannot be set to lower value than 6.
```

```
# minlen = 8

#

# The maximum credit for having digits in the new password. If le
ss than 0

# it is the minimum number of digits in the new password.

# dcredit = 0

#

# The maximum credit for having uppercase characters in the new p
assword.

# If less than 0 it is the minimum number of uppercase characters
 in the new

# password.

# ucredit = 0

#

# The maximum credit for having lowercase characters in the new p
assword.

# If less than 0 it is the minimum number of lowercase characters
 in the new

# password.

# lcredit = 0

#

# The maximum credit for having other characters in the new passw
ord.
```

```
# If less than 0 it is the minimum number of other characters in
the new

# password.

# ocredit = 0

#

# The minimum number of required classes of characters for the ne
w

# password (digits, uppercase, lowercase, others).

# minclass = 0

#

# The maximum number of allowed consecutive same characters in th
e new password.

# The check is disabled if the value is 0.

# maxrepeat = 0

#

# The maximum number of allowed consecutive characters of the sam
e class in the

# new password.

# The check is disabled if the value is 0.

# maxclassrepeat = 0

#

# Whether to check for the words from the passwd entry GECOS stri
ng of the user.
```

```
# The check is enabled if the value is not 0.

# gecoscheck = 0

#

# Whether to check for the words from the cracklib dictionary.

# The check is enabled if the value is not 0.

# dictcheck = 1

#

# Whether to check if it contains the user name in some form.

# The check is enabled if the value is not 0.

# usercheck = 1

#

# Whether the check is enforced by the PAM module and possibly ot
her

# applications.

# The new password is rejected if it fails the check and the valu
e is not 0.

# enforcing = 1

#

# Path to the cracklib dictionaries. Default is to use the crackl
ib default.

# dictpath =
```

```
minlen = 14

dcredit = -1

ucredit = -1

ocredit = -1

lcredit = -1



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

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

5.3.2
Ensure lockout for failed password attempts is configured

Not Scored
Level 1 Server
Level 1 Workstation

Result	CHEK
Message	failed password lockout configured
Time Taken	0.044817209243774414 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 fi
les,

# and should contain a list of the authentication modules that de
fine

# the central authentication scheme for use on the system

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

# traditional Unix authentication mechanisms.

#
```

```
# As of pam 1.0.1-6, this file is managed by pam-auth-update by d
efault.

# 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 s
uccess 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
```

```
auth required pam_tally2.so onerr=fail audit silent deny=5 unlock
_time=900



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	CHEK
Message	password reuse is limited
Time Taken	0.03520703315734863 seconds

Explanation:

```
Verify remembered password history is 5or more

password required pam_pwhistory.so remember=5


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	0.055899620056152344 seconds

Explanation:

```
ensure the sha512 option is included in all results

# The "sha512" option enables salted SHA512 passwords.  Without t
his option,

password     [success=1 default=ignore]     pam_unix.so obscure u
se_authtok try_first_pass 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	users password expiration not found
Time Taken	0.03463482856750488 seconds

Explanation:

```
verify PASS_MAX_DAYS conforms to site policy

#     PASS_MAX_DAYS     Maximum number of days a password may be
used.

PASS_MAX_DAYS 365



Users PASS_MAX_DAYS
```

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	0.018632411956787 11 seconds

Explanation:

```
#     PASS_MIN_DAYS     Minimum number of days allowed between pa
ssword changes.

PASS_MIN_DAYS 1
```

5.4.1.3
Ensure password expiration warning days is 7 or more

Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	users password warn not found
Time Taken	0.03372693061828613 seconds

Explanation:

```
verify PASS_WARN_AGE conforms to site policy

#     PASS_WARN_AGE     Number of days warning given before a pas
sword expires.

PASS_WARN_AGE 7



Users PASS_WARN_AGE
```

5.4.1.4
Ensure inactive password lock is 30 days or less

Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	users password lock not found
Time Taken	0.039915561676025 39 seconds

Explanation:

```
verify INACTIVE conforms to site policy

INACTIVE=30



Users INACTIVE
```

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	1.1247258186340332 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	1.6856648921966553 seconds

Explanation:

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	0.020681619644165 04 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	0.015732765197753906 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	0.020792007446289062 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	0.020422697067260742 seconds

Explanation:

```
check if following are valid terminals that may be logged in dire
ctly as root

# /etc/securetty: list of terminals on which root is allowed to l
ogin.

# 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
```

```
#...


# Comtrol 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 IO8+ serial card
ttyW0
ttyW1
#...


# Comtrol 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

ttyO0

ttyO1

```
ttyO2

ttyO3


# 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

hvsi0

hvsi1

hvsi2



# 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	0.01954174041748047 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	7.987022399902344e-05 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	0.02039647102355957 seconds

Explanation:

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

Access: 2021-08-02 06:55:54.542030156 +0000
```

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	0.0300021171569824 22 seconds

Explanation:

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

Access: 2021-08-02 06:55:54.794030752 +0000
```

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	0.027677297592163086 seconds

Explanation:

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

Access: 2021-08-02 06:55:54.794030752 +0000
```

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	0.025877714157104492 seconds

Explanation:

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

Access: 2021-08-02 06:55:54.402029825 +0000
```

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	0.019161224365234375 seconds

Explanation:

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

Access: 2021-08-02 06:46:34.000000000 +0000
```

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	0.027287483215332 03 seconds

Explanation:

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

Access: 2021-08-02 06:46:41.000000000 +0000
```

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	0.019725084304809 57 seconds

Explanation:

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

Access: 2021-08-02 06:46:34.000000000 +0000
```

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	0.030308008193969727 seconds

Explanation:

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

Access: 2021-08-02 06:55:54.000000000 +0000
```

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	2.128880500793457 seconds

Explanation:

```
running df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{
}' find '{}' -xdev -type f -perm -0002 confirms that all world wr
itable 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	5.446353435516357 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	4.663995981216431 seconds

Explanation:

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

6.1.13
Audit SUID executables

Not Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	SUID executables found
Time Taken	1.925586223602295 seconds

Explanation:

```
The following SUID executables exist

/sbin/mount.cifs

/bin/mount

/bin/fusermount

/bin/umount

/bin/ping

/bin/su

/usr/sbin/nullmailer-queue

/usr/bin/newgrp

/usr/bin/chsh

/usr/bin/chfn

/usr/bin/newgidmap
```

```
/usr/bin/sudo

/usr/bin/gpasswd

/usr/bin/pkexec

/usr/bin/mailq

/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/dmcrypt-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
```

6.1.14
Audit SGID executables

Not Scored
Level 1 Server
Level 1 Workstation

Result	FAIL
Message	SGID executables found
Time Taken	1.9266459941864014 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/ssh-agent

/usr/bin/dotlockfile

/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	0.018522500991821 29 seconds

Explanation:

```
awk -F: '($2 == "" ) { print $1 " does not have a password "}' /e
tc/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	0.019521951675415 04 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	0.03240346908569336 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	0.0199015140533447 27 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	0.025234460830688477 seconds

Explanation:

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

root
```

6.2.6
Ensure root PATH Integrity

Scored
Level 1 Server
Level 1 Workstation

Result	PASS
Message	root PATH Integrity maintained
Time Taken	0.6442432403564453 seconds

Explanation:

executing https://github.com/Deepak710/SeBAz/blob/master/linux/scripts/ind/6_2_6.sh returned the following

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	0.13591694831848145 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	0.3855910301208496 seconds

Explanation:

```
The following users have Group or world-writable home directories


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

Other Execute permission set on the home directory (/home/azureus
er) of user azureuser
```

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	0.1639096736907959 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	0.6466934680938721 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	0.13543462753295898 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	0.1260364055633545 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	0.11643671989440918 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	0.12271857261657715 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	0.28728151321411133 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	0.11320281028747559 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	0.11646103858947754 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	0.1160132884979248 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	0.1136620044708252 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	0.021999597549438477 seconds

Explanation:

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