debian 11

Report generated by Nessus™ Tue, 01 Aug 2023 09:44:34 +08

TABLE OF CONTENTS

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Compliance 'FAILED'

1.1.1.1 Ensure mounting of freevxfs filesystems is disabled - modprobe

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/freevxfs.conf and add the following line:

install freevxfs /bin/true

Run the following command to unload the freevxfs module:

rmmod freevxfs

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/modprobe -n -v freevxfs | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}'

expect: install /bin/true system: Linux

Hosts

192.168.56.115

```
The command '/sbin/modprobe -n -v freevxfs | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}''
 returned :

insmod /lib/modules/6.1.0-10-amd64/kernel/fs/freevxfs/freevxfs.ko
```

1.1.1.2 Ensure mounting of jffs2 filesystems is disabled - modprobe

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/jffs2.conf and add the following line:

install jffs2 /bin/true

Run the following command to unload the jffs2 module:

rmmod jffs2

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/modprobe -n -v jffs2 | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}'

expect: install /bin/true system: Linux

Hosts

192.168.56.115

```
The command '/sbin/modprobe -n -v jffs2 | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}''
 returned :

insmod /lib/modules/6.1.0-10-amd64/kernel/drivers/mtd/mtd.ko
insmod /lib/modules/6.1.0-10-amd64/kernel/fs/jffs2/jffs2.ko
```

1.1.1.3 Ensure mounting of hfs filesystems is disabled - modprobe

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/hfs.conf and add the following line:

install hfs /bin/true

Run the following command to unload the hfs module:

rmmod hfs

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/modprobe -n -v hfs | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}'

expect: install /bin/true system: Linux

Hosts

192.168.56.115

```
The command '/sbin/modprobe -n -v hfs | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}''
 returned :

insmod /lib/modules/6.1.0-10-amd64/kernel/fs/hfs/hfs.ko
```

1.1.1.4 Ensure mounting of hfsplus filesystems is disabled - modprobe

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/hfsplus.conf and add the following line:

install hfsplus /bin/true

Run the following command to unload the hfsplus module:

rmmod hfsplus

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/modprobe -n -v hfsplus | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}'

expect: install /bin/true system: Linux

Hosts

192.168.56.115

```
The command '/sbin/modprobe -n -v hfsplus  | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}''
 returned :

insmod /lib/modules/6.1.0-10-amd64/kernel/fs/hfsplus/hfsplus.ko
```

1.1.1.5 Ensure mounting of squashfs filesystems is disabled - modprobe

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/squashfs.conf and add the following line:

install squashfs /bin/true

Run the following command to unload the squashfs module:

rmmod squashfs

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/modprobe -n -v squashfs | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}'

expect: install /bin/true system: Linux

Hosts

192.168.56.115

```
The command '/sbin/modprobe -n -v squashfs | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}''
 returned :

insmod /lib/modules/6.1.0-10-amd64/kernel/fs/squashfs/squashfs.ko
```

1.1.1.6 Ensure mounting of udf filesystems is disabled - modprobe

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/udf.conf and add the following line:

install udf /bin/true

Run the following command to unload the udf module:

rmmod udf

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/modprobe -n -v udf | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}'

expect: install /bin/true system: Linux

Hosts

192.168.56.115

```
The command '/sbin/modprobe -n -v udf | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}''
 returned :

insmod /lib/modules/6.1.0-10-amd64/kernel/lib/crc-itu-t.ko
insmod /lib/modules/6.1.0-10-amd64/kernel/fs/udf/udf.ko
```

1.1.2 Ensure /tmp is configured - mount

Info

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

Rationale:

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

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

Solution

Configure /etc/fstab as appropriate.

example:

tmpfs/tmptmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0

OR Run the following commands to enable systemd /tmp mounting:

systemctl unmask tmp.mount systemctl enable tmp.mount

Edit /etc/systemd/system/local-fs.target.wants/tmp.mount to configure the /tmp mount:

[Mount] What=tmpfs Where=/tmp Type=tmpfs Options=mode=1777,strictatime,noexec,nodev,nosuid

Impact:

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

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

/tmp utalizing tmpfs can be resized using the size={size} parameter on the Options line on the tmp.mount file

References:

AJ Lewis, 'LVM HOWTO', http://tldp.org/HOWTO/LVM-HOWTO/

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

Notes:

If an entry for /tmp exists in /etc/fstab it will take precedence over entries in the tmp.mount file

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep /tmp expect: .*on[\s]+/tmp[\s]+type.* system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep /tmp' did not return any result
```

1.1.2 Ensure /tmp is configured - systemctl

Info

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

Rationale:

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

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

Solution

Configure /etc/fstab as appropriate.

example:

tmpfs/tmptmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0

OR Run the following commands to enable systemd /tmp mounting:

systemctl unmask tmp.mount systemctl enable tmp.mount

Edit /etc/systemd/system/local-fs.target.wants/tmp.mount to configure the /tmp mount:

[Mount] What=tmpfs Where=/tmp Type=tmpfs Options=mode=1777,strictatime,noexec,nodev,nosuid

Impact:

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

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

/tmp utalizing tmpfs can be resized using the size={size} parameter on the Options line on the tmp.mount file

References:

AJ Lewis, 'LVM HOWTO', http://tldp.org/HOWTO/LVM-HOWTO/

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

Notes:

If an entry for /tmp exists in /etc/fstab it will take precedence over entries in the tmp.mount file

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/systemctl is-enabled tmp.mount expect: enabled system: Linux

Hosts

192.168.56.115

```
The command '/bin/systemctl is-enabled tmp.mount' returned :

Failed to get unit file state for tmp.mount: No such file or directory
```

1.1.3 Ensure nodev option set on /tmp partition

Info

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

Rationale:

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

Solution

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

Run the following command to remount /tmp :

mount -o remount,nodev /tmp

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

[Mount] Options=mode=1777,strictatime,noexec,nodev,nosuid

Run the following command to remount /tmp :

mount -o remount,nodev /tmp

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep /tmp expect: [\s]*[,]?nodev system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep /tmp' did not return any result
```

1.1.4 Ensure nosuid option set on /tmp partition

Info

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

Rationale:

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

Solution

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

Run the following command to remount /tmp :

mount -o remount,nosuid /tmp

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

[Mount] Options=mode=1777,strictatime,noexec,nodev,nosuid

Run the following command to remount /tmp :

mount -o remount,nosuid /tmp

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep /tmp expect: [\s]*[,]?nosuid system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep /tmp' did not return any result
```

1.1.5 Ensure noexec option set on /tmp partition

Info

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

Rationale:

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

Solution

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

Run the following command to remount /tmp :

mount -o remount,noexec /tmp

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

[Mount] Options=mode=1777,strictatime,noexec,nodev,nosuid

Run the following command to remount /tmp :

mount -o remount,noexec /tmp

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.9
800-53	CM-11
800-53R5	CM-11
CSCV7	2.6
CSF	DE.CM-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.2
LEVEL	1S
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep /tmp expect: [\s]*[,]?noexec system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep /tmp' did not return any result
```

1.1.8 Ensure nodev option set on /var/tmp partition

Info

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

Rationale:

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

Solution

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

Run the following command to remount /var/tmp :

mount -o remount,nodev /var/tmp

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep /var/tmp expect: [\s]*[,]?nodev system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep /var/tmp' did not return any result
```

1.1.9 Ensure nosuid option set on /var/tmp partition

Info

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

Rationale:

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

Solution

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

Run the following command to remount /var/tmp :

mount -o remount,nosuid /var/tmp

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep /var/tmp expect: [\s]*[,]?nosuid system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep /var/tmp' did not return any result
```

1.1.10 Ensure noexec option set on /var/tmp partition

Info

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

Rationale:

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

Solution

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

Run the following command to remount /var/tmp :

mount -o remount,noexec /var/tmp

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.9
800-53	CM-11
800-53R5	CM-11
CSCV7	2.6
CSF	DE.CM-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.2
LEVEL	1S
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep /var/tmp expect: [\s]*[,]?noexec system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep /var/tmp' did not return any result
```

1.1.14 Ensure nodev option set on /home partition

Info

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

Rationale:

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

Solution

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

mount -o remount,nodev /home

Notes:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep /home expect: [\s]*[,]?nodev system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep /home' did not return any result
```

1.1.17 Ensure noexec option set on /dev/shm partition

Info

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

Rationale:

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

Solution

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

Run the following command to remount /dev/shm:

mount -o remount,noexec /dev/shm

Notes:

The setting in /etc/default/rcS, if present, will still be used, but the setting in /etc/default/tmpfs will take precedence if enabled. If desired, the defaults may also be overridden with an entry in in /etc/fstab

/run/shm was previously /dev/shm, and a compatibility symlink or bind mount will be created to allow the old path to continue to function. If an fstab entry for /dev/shm exists instead of /run/shm, then /dev/shm will continue to be used.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.9
800-53	CM-11
800-53R5	CM-11
CSCV7	2.6
CSF	DE.CM-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.2
LEVEL	1S
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep /dev/shm expect: [\s]*[,]?noexec system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep /dev/shm' returned :

tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
```

1.1.18 Ensure nodev option set on removable media partitions

Info

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

Rationale:

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

Solution

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1NS
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep -P 'on[\s]+/dev/(floppy|cdrom|corder|mmcblk)'

expect: nodev system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep -P 'on[\s]+/dev/(floppy|cdrom|corder|mmcblk)'' did not return
 any result
```

1.1.19 Ensure nosuid option set on removable media partitions

Info

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

Rationale:

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

Solution

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1NS
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep -P 'on[\s]+/dev/(floppy|cdrom|corder|mmcblk)'

expect: nosuid system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep -P 'on[\s]+/dev/(floppy|cdrom|corder|mmcblk)'' did not return
 any result
```

1.1.20 Ensure noexec option set on removable media partitions

Info

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

Rationale:

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

Solution

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.9
800-53	CM-11
800-53R5	CM-11
CSCV7	2.6
CSF	DE.CM-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.2
LEVEL	1NS
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep -P 'on[\s]+/dev/(floppy|cdrom|corder|mmcblk)'

expect: noexec system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep -P 'on[\s]+/dev/(floppy|cdrom|corder|mmcblk)'' did not return
 any result
```

1.1.23 Disable USB Storage - modprobe

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/usb_storage.conf and add the following line:

install usb-storage /bin/true

Run the following command to unload the usb-storage module:

rmmod usb-storage

Notes:

An alternative solution to disabling the usb-storage module may be found in USBGuard.

Use of USBGuard and construction of USB device policies should be done in alignment with site policy.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.2
800-171	3.14.4
800-171	3.14.5
800-53	SI-3
800-53R5	SI-3
CN-L3	7.1.3.6(b)
CN-L3	8.1.4.5
CN-L3	8.1.9.6(a)
CN-L3	8.1.9.6(b)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.7(a)
CN-L3	8.1.10.7(b)
CSCV6	3.1

CSCV7	8.4
CSCV7	8.5
CSF	DE.CM-4
CSF	DE.DP-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.2.1
ITSG-33	SI-3
LEVEL	1S
NIAV2	GS8a
PCI-DSSV3.2.1	5.1
PCI-DSSV3.2.1	5.1.1
PCI-DSSV4.0	5.2.1
QCSC-V1	3.2
QCSC-V1	5.2.3
QCSC-V1	8.2.1
TBA-FIISB	49.2.1
TBA-FIISB	49.2.2
TBA-FIISB	49.3.1
TBA-FIISB	49.3.2
TBA-FIISB	50.2.1
TBA-FIISB	51.2.4
TBA-FIISB	51.2.7

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/modprobe -n -v usb-storage | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}'

expect: install /bin/true system: Linux

Hosts

192.168.56.115

```
The command '/sbin/modprobe -n -v usb-storage | /usr/bin/awk '{print} END {if (NR == 0) print
 "fail"}'' returned :

insmod /lib/modules/6.1.0-10-amd64/kernel/drivers/usb/storage/usb-storage.ko
```

1.3.3 Ensure sudo log file exists

Info

sudo can use a custom log file

Rationale:

A sudo log file simplifies auditing of sudo commands

Solution

edit the file /etc/sudoers or a file in /etc/sudoers.d/ with visudo -f and add the following line: and add the following line:

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

Example

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

Notes:

visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks or parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-12
800-53R5	AU-12
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-12
LEVEL	1S
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2

QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*Defaults[[:space:]]+([^#]+,[[:space:]]*)?logfile=' /etc/sudoers /etc/sudoers.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*Defaults[[:space:]]+([^#]+,[[:space:]]*)?logfile=' /
etc/sudoers /etc/sudoers.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print
 "fail"}'' returned :

fail
```

1.4.1 Ensure AIDE is installed

Info

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

Rationale:

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

Solution

Install AIDE using the appropriate package manager or manual installation:

apt install aide aide-common

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

aideinit

Notes:

The prelinking feature can interfere with AIDE because it alters binaries to speed up their start up times. Run prelink -ua to restore the binaries to their prelinked state, thus avoiding false positives from AIDE.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53R5	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV6	2.2
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)

ITSG-33	AU-3
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s aide 2>&1 expect: install[\s]+ok[\s]+installed system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s aide 2>&1' returned :

dpkg-query: package 'aide' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

1.4.2 Ensure filesystem integrity is regularly checked

Info

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

Rationale:

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

Solution

If cron will be used to schedule and run aide check Run the following command:

crontab -u root -e

Add the following line to the crontab:

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

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

[Unit] Description=Aide Check

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

[Install] WantedBy=multi-user.target

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

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

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

[Install] WantedBy=multi-user.target

Run the following commands:

chown root:root /etc/systemd/system/aidecheck.* # chmod 0644 /etc/systemd/system/aidecheck.*

systemctl daemon-reload

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

References:

https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.service https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.timer

Notes:

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

Note that Debian advises using /usr/bin/aide.wrapper rather than calling /usr/bin/aide directly in order to protect the database and prevent conflicts.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53R5	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

FAILED

Hosts

192.168.56.115

1.5.2 Ensure bootloader password is set - password_pbkdf2

Info

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

Rationale:

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

Solution

Create an encrypted password with grub-mkpasswd-pbkdf2:

grub-mkpasswd-pbkdf2 Enter password: <password>

Reenter password: <password>

PBKDF2 hash of your password is <encrypted-password>

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

cat <<EOF set superusers='<username>'

password_pbkdf2 <username> <encrypted-password>

EOF

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

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

CLASS='--class gnu-linux --class gnu --class os --unrestricted'

Run the following command to update the grub2 configuration:

update-grub

Impact:

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

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

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

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

Notes:

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

Replace /boot/grub/grub.cfg with the appropriate grub configuration file for your environment.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*password_pbkdf2[\s]+[^\s]+[\s]+[^\s]+[\s]*$ file: /boot/grub/grub.cfg regex: ^[\s]*password system: Linux

Hosts

192.168.56.115

```
The file "/boot/grub/grub.cfg" does not contain "^[\s]*password"
```

1.5.2 Ensure bootloader password is set - set superusers

Info

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

Rationale:

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

Solution

Create an encrypted password with grub-mkpasswd-pbkdf2:

grub-mkpasswd-pbkdf2 Enter password: <password>

Reenter password: <password>

PBKDF2 hash of your password is <encrypted-password>

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

cat <<EOF set superusers='<username>'

password_pbkdf2 <username> <encrypted-password>

EOF

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

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

CLASS='--class gnu-linux --class gnu --class os --unrestricted'

Run the following command to update the grub2 configuration:

update-grub

Impact:

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

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

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

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

Notes:

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

Replace /boot/grub/grub.cfg with the appropriate grub configuration file for your environment.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*set[\s]*superusers[\s]*=".+"*$ file: /boot/grub/grub.cfg regex: ^[\s]*set[\s]*superusers[\s]*= system: Linux

Hosts

192.168.56.115

```
The file "/boot/grub/grub.cfg" does not contain "^[\s]*set[\s]*superusers[\s]*="
```

1.6.2 Ensure address space layout randomization (ASLR) is enabled

Info

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

Rationale:

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

Solution

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

kernel.randomize_va_space = 2

Run the following command to set the active kernel parameter:

sysctl -w kernel.randomize_va_space=2

See Also

https://workbench.cisecurity.org/files/2658

References

800-53	SC-39
800-53	SI-16
800-53R5	SC-39
800-53R5	SI-16
CSCV7	8.3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
LEVEL	1S
QCSC-V1	5.2.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -P '^[\s]*kernel\.randomize_va_space[\s]*=[\s]*2[\s]*$' /etc/sysctl.conf /etc/sysctl.d/* |/ usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -P '^[\s]*kernel\.randomize_va_space[\s]*=[\s]*2[\s]*$' /etc/sysctl.conf /
etc/sysctl.d/* |/usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}''
 returned :

fail
```

1.6.4 Ensure core dumps are restricted - /etc/sysctl.conf

Info

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

Rationale:

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

Solution

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

* hard core 0

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

fs.suid_dumpable = 0

Run the following command to set the active kernel parameter:

sysctl -w fs.suid_dumpable=0

If systemd-coredump is installed:

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

Storage=none ProcessSizeMax=0

Run the command:

systemctl daemon-reload

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6

LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/grep -s -E '^[[:space:]]*fs\.suid_dumpable[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/grep -s -E '^[[:space:]]*fs
\.suid_dumpable[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/
awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

1.6.4 Ensure core dumps are restricted - limits.conf limits.d

Info

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

Rationale:

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

Solution

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

* hard core 0

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

fs.suid_dumpable = 0

Run the following command to set the active kernel parameter:

sysctl -w fs.suid_dumpable=0

If systemd-coredump is installed:

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

Storage=none ProcessSizeMax=0

Run the command:

systemctl daemon-reload

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6

LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]**[[:space:]]+hard[[:space:]]+core[[:space:]]+0[[:space:]]*$' /etc/security/limits.conf /etc/security/limits.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*
\*[[:space:]]+hard[[:space:]]+core[[:space:]]+0[[:space:]]*$' /etc/security/limits.conf /etc/
security/limits.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}''
 returned :

fail
```

1.7.1.2 Ensure AppArmor is enabled in the bootloader configuration - apparmor=1

Info

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

Rationale:

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

Solution

edit /etc/default/grub and add the appermor=1 and security=apparmor parameters to the GRUB_CMDLINE_LINUX= line

GRUB_CMDLINE_LINUX='apparmor=1 security=apparmor'

Run the following command to update the grub2 configuration:

update-grub

Notes:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: [\s]*[Aa][Pp][Pp][Aa][Rr][Mm][Oo][Rr][\s]*=[\s]*1 file: /boot/grub/grub.cfg regex: ^[\s]*linux.* system: Linux

Hosts

192.168.56.115

```
Non-compliant file(s):
      /boot/grub/grub.cfg - regex '^[\s]*linux.*' found - expect '[\s]*[Aa][Pp][Pp][Aa][Rr][Mm][Oo]
[Rr][\s]*=[\s]*1' not found in the following lines:
          133: linux/boot/vmlinuz-6.1.0-10-amd64 root=UUID=304ac076-382a-4acf-8aea-319fe7666a7f ro
 quiet
          151: linux/boot/vmlinuz-6.1.0-10-amd64 root=UUID=304ac076-382a-4acf-8aea-319fe7666a7f ro
 quiet
          168: linux/boot/vmlinuz-6.1.0-10-amd64 root=UUID=304ac076-382a-4acf-8aea-319fe7666a7f ro
 single
```

1.7.1.2 Ensure AppArmor is enabled in the bootloader configuration - security=apparmor

Info

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

Rationale:

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

Solution

edit /etc/default/grub and add the appermor=1 and security=apparmor parameters to the GRUB_CMDLINE_LINUX= line

GRUB_CMDLINE_LINUX='apparmor=1 security=apparmor'

Run the following command to update the grub2 configuration:

update-grub

Notes:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: [\s]*[Ss][Ee][Cc][Uu][Rr][Ii][Tt][Yy][\s]*=[\s]*[Aa][Pp][Pp][Aa][Rr][Mm][Oo][Rr] file: /boot/grub/grub.cfg regex: ^[\s]*linux.* system: Linux

Hosts

192.168.56.115

```
Non-compliant file(s):
      /boot/grub/grub.cfg - regex '^[\s]*linux.*' found - expect '[\s]*[Ss][Ee][Cc][Uu][Rr][Ii][Tt]
[Yy][\s]*=[\s]*[Aa][Pp][Pp][Aa][Rr][Mm][Oo][Rr]' not found in the following lines:
          133: linux/boot/vmlinuz-6.1.0-10-amd64 root=UUID=304ac076-382a-4acf-8aea-319fe7666a7f ro
 quiet
          151: linux/boot/vmlinuz-6.1.0-10-amd64 root=UUID=304ac076-382a-4acf-8aea-319fe7666a7f ro
 quiet
          168: linux/boot/vmlinuz-6.1.0-10-amd64 root=UUID=304ac076-382a-4acf-8aea-319fe7666a7f ro
 single
```

1.8.1.1 Ensure message of the day is configured properly

Info

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

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

Rationale:

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

Solution

Edit the /etc/motd file with the appropriate contents according to your site policy, remove any instances of m , r , s , v or references to the OS platform OR If the motd is not used, this file can be removed.

Run the following command to remove the motd file:

rm /etc/motd

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: (\\[mrsv]|[Dd]ebian) file: /etc/motd regex: (\\[mrsv]|[Dd]ebian) required: NO system: Linux

Hosts

192.168.56.115

```
Non-compliant file(s):
      /etc/motd - regex '(\\[mrsv]|[Dd]ebian)' found - expect '(\\[mrsv]|[Dd]ebian)' found in the
 following lines:
          2: The programs included with the Debian GNU/Linux system are free software;
          6: Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
```

1.8.1.2 Ensure local login warning banner is configured properly

Info

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

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

Rationale:

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

Solution

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

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: (\\[mrsv]|[Dd]ebian) file: /etc/issue regex: (\\[mrsv]|[Dd]ebian) required: NO system: Linux

Hosts

192.168.56.115

```
Non-compliant file(s):
      /etc/issue - regex '(\\[mrsv]|[Dd]ebian)' found - expect '(\\[mrsv]|[Dd]ebian)' found in the
 following lines:
          1: Debian GNU/Linux 12 \n \l
```

1.8.1.3 Ensure remote login warning banner is configured properly

Info

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

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

Rationale:

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

Solution

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

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: (\\[mrsv]|[Dd]ebian) file: /etc/issue.net regex: (\\[mrsv]|[Dd]ebian) required: NO system: Linux

Hosts

192.168.56.115

```
Non-compliant file(s):
      /etc/issue.net - regex '(\\[mrsv]|[Dd]ebian)' found - expect '(\\[mrsv]|[Dd]ebian)' found in
 the following lines:
          1: Debian GNU/Linux 12
```

1.8.2 Ensure GDM login banner is configured - banner message enabled

Info

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

Rationale:

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

Solution

Edit or create the file /etc/gdm3/greeter.dconf-defaults and add the following:

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

Notes:

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

If a different GUI login service is in use, consult your documentation and apply an equivalent banner.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*banner-message-enable[\s]*=[\s]*true[\s]*$ file: /etc/gdm3/greeter.dconf-defaults regex: ^[\s]*banner-message-enable[\s]*= system: Linux

Hosts

192.168.56.115

```
The file "/etc/gdm3/greeter.dconf-defaults" does not contain "^[\s]*banner-message-enable[\s]*="
```

1.8.2 Ensure GDM login banner is configured - banner text

Info

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

Rationale:

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

Solution

Edit or create the file /etc/gdm3/greeter.dconf-defaults and add the following:

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

Notes:

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

If a different GUI login service is in use, consult your documentation and apply an equivalent banner.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

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

Hosts

192.168.56.115

```
First ERROR: # Automatic suspend != Authorized uses
# These are the options for the greeter session that can be set
# through GSettings. Any GSettings setting that is used by the
# greeter session can be set here.

# Note that you must configure the path used by dconf to store the
# configuration, not the GSettings path.


# Theming options
# ===============
#  - Change the GTK+ theme
[org/gnome/desktop/interface]
# gtk-theme='Adwaita'
#  - Use another background
[org/gnome/desktop/background]
# picture-uri='file:///usr/share/themes/Adwaita/backgrounds/stripes.jpg'
# picture-options='zoom'
#  - Or no background at all
[org/gnome/desktop/background]
# picture-options='none'
# primary-color='#000000'

# Login manager options
# =====================
[org/gnome/login-screen]
logo='/usr/share/images/vendor-logos/logo-text-version-64.png'

# - Disable user list
# disable-user-list=true
# - Disable restart buttons
# disable-restart-buttons=true
# - Show a login welcome message
# banner-message-enable=true
# banner-message-text='Welcome'

# Automatic suspend
# =================
[org/gnome/settings-daemon/plugins/power]
# - Time inactive in seconds before suspending with AC power
#   1200=20 minutes, 0=never
# sleep-inactive-ac-timeout=1200
# - What to do after sleep-inactive-ac-timeout
#   'blank', 'suspend', 'shutdown', 'hibernate', 'interactive' or 'nothing'
# sleep-inactive-ac-type='suspend'
# - As above but when on battery
# sleep-inactive-battery-timeout=1200
# sleep-inactive-battery-type='suspend'
```

2.2.1.2 Ensure systemd-timesyncd is configured - FallbackNTP

Info

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network. It implements an SNTP client. In contrast to NTP implementations such as chrony or the NTP reference server this only implements a client side, and does not bother with the full NTP complexity, focusing only on querying time from one remote server and synchronizing the local clock to it. The daemon runs with minimal privileges, and has been hooked up with networkd to only operate when network connectivity is available. The daemon saves the current clock to disk every time a new NTP sync has been acquired, and uses this to possibly correct the system clock early at bootup, in order to accommodate for systems that lack an RTC such as the Raspberry Pi and embedded devices, and make sure that time monotonically progresses on these systems, even if it is not always correct. To make use of this daemon a new system user and group 'systemd-timesync' needs to be created on installation of systemd.

Note: The systemd-timesyncd service specifically implements only SNTP. This minimalistic service will set the system clock for large offsets or slowly adjust it for smaller deltas. More complex use cases are not covered by systemd-timesyncd.

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

Rationale:

Proper configuration is vital to ensuring time synchronization is working properly.

Solution

Run the following command to enable systemd-timesyncd

systemctl enable systemd-timesyncd.service

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

NTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org #Servers listed should be In Accordence With Local Policy

FallbackNTP=2.debian.pool.ntp.org 3.debian.pool.ntp.org #Servers listed should be In Accordence With Local Policy

RootDistanceMax=1 #should be In Accordence With Local Policy

Run the following commands to start systemd-timesyncd.service

systemctl start systemd-timesyncd.service

timedatectl set-ntp true

Notes:

some versions of systemd have been compiled without systemd-timesycnd. On these distributions, chrony or NTP should be used instead of systemd-timesycnd.

Not all options are avalible on all versions of systemd-timesyncd

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.7
800-53	AU-8
800-53R5	AU-8
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1NS
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: grep -e 'FallbackNTP=' /etc/systemd/timesyncd.conf expect: ^[s]*FallbackNTP=10\.0\.0\.2 system: Linux

Hosts

192.168.56.115

```
The command 'grep -e 'FallbackNTP=' /etc/systemd/timesyncd.conf' returned :

#FallbackNTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org 2.debian.pool.ntp.org 3.debian.pool.ntp.org
```

2.2.1.2 Ensure systemd-timesyncd is configured - NTP

Info

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network. It implements an SNTP client. In contrast to NTP implementations such as chrony or the NTP reference server this only implements a client side, and does not bother with the full NTP complexity, focusing only on querying time from one remote server and synchronizing the local clock to it. The daemon runs with minimal privileges, and has been hooked up with networkd to only operate when network connectivity is available. The daemon saves the current clock to disk every time a new NTP sync has been acquired, and uses this to possibly correct the system clock early at bootup, in order to accommodate for systems that lack an RTC such as the Raspberry Pi and embedded devices, and make sure that time monotonically progresses on these systems, even if it is not always correct. To make use of this daemon a new system user and group 'systemd-timesync' needs to be created on installation of systemd.

Note: The systemd-timesyncd service specifically implements only SNTP. This minimalistic service will set the system clock for large offsets or slowly adjust it for smaller deltas. More complex use cases are not covered by systemd-timesyncd.

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

Rationale:

Proper configuration is vital to ensuring time synchronization is working properly.

Solution

Run the following command to enable systemd-timesyncd

systemctl enable systemd-timesyncd.service

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

NTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org #Servers listed should be In Accordence With Local Policy

FallbackNTP=2.debian.pool.ntp.org 3.debian.pool.ntp.org #Servers listed should be In Accordence With Local Policy

RootDistanceMax=1 #should be In Accordence With Local Policy

Run the following commands to start systemd-timesyncd.service

systemctl start systemd-timesyncd.service

timedatectl set-ntp true

Notes:

some versions of systemd have been compiled without systemd-timesycnd. On these distributions, chrony or NTP should be used instead of systemd-timesycnd.

Not all options are avalible on all versions of systemd-timesyncd

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.7
800-53	AU-8
800-53R5	AU-8
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1NS
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: grep -e 'NTP=' /etc/systemd/timesyncd.conf expect: ^[s]*NTP=192\.168\.0\.1 system: Linux

Hosts

192.168.56.115

```
The command 'grep -e 'NTP=' /etc/systemd/timesyncd.conf' returned :

#NTP=
#FallbackNTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org 2.debian.pool.ntp.org 3.debian.pool.ntp.org
```

2.2.1.2 Ensure systemd-timesyncd is configured - RootDistanceMax

Info

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network. It implements an SNTP client. In contrast to NTP implementations such as chrony or the NTP reference server this only implements a client side, and does not bother with the full NTP complexity, focusing only on querying time from one remote server and synchronizing the local clock to it. The daemon runs with minimal privileges, and has been hooked up with networkd to only operate when network connectivity is available. The daemon saves the current clock to disk every time a new NTP sync has been acquired, and uses this to possibly correct the system clock early at bootup, in order to accommodate for systems that lack an RTC such as the Raspberry Pi and embedded devices, and make sure that time monotonically progresses on these systems, even if it is not always correct. To make use of this daemon a new system user and group 'systemd-timesync' needs to be created on installation of systemd.

Note: The systemd-timesyncd service specifically implements only SNTP. This minimalistic service will set the system clock for large offsets or slowly adjust it for smaller deltas. More complex use cases are not covered by systemd-timesyncd.

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

Rationale:

Proper configuration is vital to ensuring time synchronization is working properly.

Solution

Run the following command to enable systemd-timesyncd

systemctl enable systemd-timesyncd.service

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

NTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org #Servers listed should be In Accordence With Local Policy

FallbackNTP=2.debian.pool.ntp.org 3.debian.pool.ntp.org #Servers listed should be In Accordence With Local Policy

RootDistanceMax=1 #should be In Accordence With Local Policy

Run the following commands to start systemd-timesyncd.service

systemctl start systemd-timesyncd.service

timedatectl set-ntp true

Notes:

some versions of systemd have been compiled without systemd-timesycnd. On these distributions, chrony or NTP should be used instead of systemd-timesycnd.

Not all options are avalible on all versions of systemd-timesyncd

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.7
800-53	AU-8
800-53R5	AU-8
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1NS
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[s]*RootDistanceMaxSec=1 file: /etc/systemd/timesyncd.conf regex: ^[s]*RootDistanceMaxSec system: Linux

Hosts

192.168.56.115

```
The file "/etc/systemd/timesyncd.conf" does not contain "^[s]*RootDistanceMaxSec"
```

2.2.3 Ensure Avahi Server is not enabled

Info

Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine.

Rationale:

Automatic discovery of network services is not normally required for system functionality. It is recommended to disable the service to reduce the potential attack surface.

Solution

Run the following command to disable avahi-daemon:

systemctl --now disable avahi-daemon

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6

CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

enabled
```

2.2.4 Ensure CUPS is not enabled

Info

The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability.

Rationale:

If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be disabled to reduce the potential attack surface.

Solution

Run one of the following commands to disable cups :

systemctl --now disable cups

Impact:

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

References:

More detailed documentation on CUPS is available at the project homepage at http://www.cups.org.

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3

CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

enabled
```

3.1.2 Ensure wireless interfaces are disabled

Info

Wireless networking is used when wired networks are unavailable. Debian contains a wireless tool kit to allow system administrators to configure and use wireless networks.

Rationale:

If wireless is not to be used, wireless devices can be disabled to reduce the potential attack surface.

Solution

Run the following command to disable any wireless interfaces:

nmcli radio all off

Impact:

Many if not all laptop workstations and some desktop workstations will connect via wireless requiring these interfaces be enabled.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.16
800-53	AC-18(3)
800-53	AC-18(4)
800-53R5	AC-18(3)
800-53R5	AC-18(4)
CSCV7	15.4
CSCV7	15.5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ITSG-33	AC-18(3)
ITSG-33	AC-18(4)
LEVEL	1S
QCSC-V1	5.2.1
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/nmcli radio wifi expect: disabled system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/nmcli radio wifi' returned :

enabled
```

3.2.1 Ensure packet redirect sending is disabled - all /etc/sysctl.conf /etc/sysctl.d/*

Info

ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects.

Rationale:

An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all\.send_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all
\.send_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.1 Ensure packet redirect sending is disabled - all sysctl

Info

ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects.

Rationale:

An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.conf.all.send_redirects expect: ^[\s]*net\.ipv4\.conf\.all \.send_redirects[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.conf.all.send_redirects' returned :

net.ipv4.conf.all.send_redirects = 1
```

3.2.1 Ensure packet redirect sending is disabled - default /etc/sysctl.conf /etc/sysctl.d/*

Info

ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects.

Rationale:

An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default\.send_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.send_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.1 Ensure packet redirect sending is disabled - default sysctl

Info

ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects.

Rationale:

An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.conf.default.send_redirects expect: ^[\s]*net\.ipv4\.conf\.default \.send_redirects[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.conf.default.send_redirects' returned :

net.ipv4.conf.default.send_redirects = 1
```

3.2.2 Ensure IP forwarding is disabled - ipv4 /etc/sysctl.conf /etc/sysctl.d/*

Info

The net.ipv4.ip_forward and net.ipv6.conf.all.forwarding flags are used to tell the system whether it can forward packets or not.

Rationale:

Setting the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Solution

Run the following command to restore the default parameter and set the active kernel parameter:

grep -Els '^s*net.ipv4.ip_forwards*=s*1' /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while read filename; do sed -ri 's/^s*(net.ipv4.ip_forwards*)(=)(s*S+b).*$/# *REMOVED* 1/' $filename; done; sysctl -w net.ipv4.ip_forward=0; sysctl -w net.ipv4.route.flush=1

IF IPv6 is enabled:

Run the following command to restore the default parameter and set the active kernel parameter:

grep -Els '^s*net.ipv6.conf.all.forwardings*=s*1' /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while read filename; do sed -ri 's/^s*(net.ipv6.conf.all.forwardings*)(=)(s*S+b).*$/# *REMOVED* 1/' $filename; done; sysctl -w net.ipv6.conf.all.forwarding=0; sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.ip_forward[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net
\.ipv4\.ip_forward[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.2 Ensure IP forwarding is disabled - ipv6 /etc/sysctl.conf /etc/sysctl.d/*

Info

The net.ipv4.ip_forward and net.ipv6.conf.all.forwarding flags are used to tell the system whether it can forward packets or not.

Rationale:

Setting the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Solution

Run the following command to restore the default parameter and set the active kernel parameter:

grep -Els '^s*net.ipv4.ip_forwards*=s*1' /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while read filename; do sed -ri 's/^s*(net.ipv4.ip_forwards*)(=)(s*S+b).*$/# *REMOVED* 1/' $filename; done; sysctl -w net.ipv4.ip_forward=0; sysctl -w net.ipv4.route.flush=1

IF IPv6 is enabled:

Run the following command to restore the default parameter and set the active kernel parameter:

grep -Els '^s*net.ipv6.conf.all.forwardings*=s*1' /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while read filename; do sed -ri 's/^s*(net.ipv6.conf.all.forwardings*)(=)(s*S+b).*$/# *REMOVED* 1/' $filename; done; sysctl -w net.ipv6.conf.all.forwarding=0; sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.all\.forwarding[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.all
\.forwarding[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk
 '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.3.1 Ensure source routed packets are not accepted - files 'net.ipv4.conf.all.accept_source_route = 0'

Info

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

Rationale:

Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6

CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all \.accept_source_route[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all
\.accept_source_route[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.3.1 Ensure source routed packets are not accepted - files 'net.ipv4.conf.default.accept_source_route = 0'

Info

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

Rationale:

Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6

CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default \.accept_source_route[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.accept_source_route[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.3.1 Ensure source routed packets are not accepted - files 'net.ipv6.conf.all.accept_source_route = 0'

Info

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

Rationale:

Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6

CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.all \.accept_source_route[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.all
\.accept_source_route[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.3.1 Ensure source routed packets are not accepted - files 'net.ipv6.conf.default.accept_source_route = 0'

Info

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

Rationale:

Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6

CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.default \.accept_source_route[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.default
\.accept_source_route[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.3.1 Ensure source routed packets are not accepted - net.ipv4.conf.default.accept_source_route = 0

Info

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

Rationale:

Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6

CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.conf.default.accept_source_route expect: ^[\s]*net\.ipv4\.conf\.default \.accept_source_route[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.conf.default.accept_source_route' returned :

net.ipv4.conf.default.accept_source_route = 1
```

3.3.2 Ensure ICMP redirects are not accepted - 'net.ipv4.conf.default.accept_redirects'

Info

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.accept_redirects to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)

ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.conf.default.accept_redirects expect: ^[\s]*net\.ipv4\.conf\.default \.accept_redirects[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.conf.default.accept_redirects' returned :

net.ipv4.conf.default.accept_redirects = 1
```

3.3.2 Ensure ICMP redirects are not accepted - 'net.ipv6.conf.default.accept_redirects'

Info

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.accept_redirects to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)

ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv6.conf.default.accept_redirects expect: ^[\s]*net\.ipv6\.conf\.default \.accept_redirects[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv6.conf.default.accept_redirects' returned :

net.ipv6.conf.default.accept_redirects = 1
```

3.3.2 Ensure ICMP redirects are not accepted - files net.ipv4.conf.all.accept_redirects= 0

Info

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.accept_redirects to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)

ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all\.accept_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all
\.accept_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.3.2 Ensure ICMP redirects are not accepted - files net.ipv4.conf.default.accept_redirects= 0

Info

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.accept_redirects to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)

ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.accept_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print}
END {if (NR != 0) print "pass"; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.accept_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.3.2 Ensure ICMP redirects are not accepted - files net.ipv6.conf.all.accept_redirects= 0

Info

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.accept_redirects to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)

ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.all\.accept_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.all
\.accept_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.3.2 Ensure ICMP redirects are not accepted - files net.ipv6.conf.default.accept_redirects= 0

Info

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.accept_redirects to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)

ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.default
\.accept_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print}
END {if (NR != 0) print "pass"; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.default
\.accept_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.3.2 Ensure ICMP redirects are not accepted - net.ipv4.conf.all.accept_redirects

Info

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.accept_redirects to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6

LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.conf.all.accept_redirects expect: ^[\s]*net\.ipv4\.conf\.all \.accept_redirects[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.conf.all.accept_redirects' returned :

net.ipv4.conf.all.accept_redirects = 1
```

3.3.3 Ensure secure ICMP redirects are not accepted - files net.ipv4.conf.all.secure_redirects = 0

Info

Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure.

Rationale:

It is still possible for even known gateways to be compromised. Setting net.ipv4.conf.all.secure_redirects to 0 protects the system from routing table updates by possibly compromised known gateways.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all\.secure_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all
\.secure_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.3.3 Ensure secure ICMP redirects are not accepted - files net.ipv4.conf.default.secure_redirects = 0

Info

Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure.

Rationale:

It is still possible for even known gateways to be compromised. Setting net.ipv4.conf.all.secure_redirects to 0 protects the system from routing table updates by possibly compromised known gateways.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.secure_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print}
END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.secure_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.3.3 Ensure secure ICMP redirects are not accepted - net.ipv4.conf.all.secure_redirects = 0

Info

Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure.

Rationale:

It is still possible for even known gateways to be compromised. Setting net.ipv4.conf.all.secure_redirects to 0 protects the system from routing table updates by possibly compromised known gateways.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.conf.all.secure_redirects expect: ^[\s]*net\.ipv4\.conf\.all \.secure_redirects[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.conf.all.secure_redirects' returned :

net.ipv4.conf.all.secure_redirects = 1
```

3.3.3 Ensure secure ICMP redirects are not accepted - net.ipv4.conf.default.secure_redirects = 0

Info

Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure.

Rationale:

It is still possible for even known gateways to be compromised. Setting net.ipv4.conf.all.secure_redirects to 0 protects the system from routing table updates by possibly compromised known gateways.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.conf.default.secure_redirects expect: ^[\s]*net\.ipv4\.conf\.default \.secure_redirects[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.conf.default.secure_redirects' returned :

net.ipv4.conf.default.secure_redirects = 1
```

3.3.4 Ensure suspicious packets are logged - files net.ipv4.conf.all.log_martians = 1

Info

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

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all\.log_martians[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all
\.log_martians[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/
awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.3.4 Ensure suspicious packets are logged - files net.ipv4.conf.default.log_martians = 1

Info

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

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default\.log_martians[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.log_martians[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/
awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.3.4 Ensure suspicious packets are logged - net.ipv4.conf.all.log_martians = 1

Info

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

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)

ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.conf.all.log_martians expect: ^[\s]*net\.ipv4\.conf\.all
\.log_martians[\s]*=[\s]*1[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.conf.all.log_martians' returned :

net.ipv4.conf.all.log_martians = 0
```

3.3.4 Ensure suspicious packets are logged - net.ipv4.conf.default.log_martians = 1

Info

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

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.conf.default.log_martians expect: ^[\s]*net\.ipv4\.conf\.default \.log_martians[\s]*=[\s]*1[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.conf.default.log_martians' returned :

net.ipv4.conf.default.log_martians = 0
```

3.3.5 Ensure broadcast ICMP requests are ignored - files net.ipv4.icmp_echo_ignore_broadcasts = 1

Info

Setting net.ipv4.icmp_echo_ignore_broadcasts to 1 will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses.

Rationale:

Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

Solution

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

net.ipv4.icmp_echo_ignore_broadcasts = 1

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1

sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net \.ipv4\.icmp_echo_ignore_broadcasts[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* |/ usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net
\.ipv4\.icmp_echo_ignore_broadcasts[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/
sysctl.d/* |/usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.3.6 Ensure bogus ICMP responses are ignored - files net.ipv4.icmp_ignore_bogus_error_responses = 1

Info

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

Rationale:

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

Solution

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

net.ipv4.icmp_ignore_bogus_error_responses = 1

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1

sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net \.ipv4\.icmp_ignore_bogus_error_responses[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net
\.ipv4\.icmp_ignore_bogus_error_responses[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /
etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}''
 returned :

fail
```

3.3.7 Ensure Reverse Path Filtering is enabled - files net.ipv4.conf.all.rp_filter = 1

Info

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

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.conf.all.rp_filter=1

sysctl -w net.ipv4.conf.default.rp_filter=1

sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all\.rp_filter[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all
\.rp_filter[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk
 '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.3.7 Ensure Reverse Path Filtering is enabled - files net.ipv4.conf.default.rp_filter = 1

Info

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

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.conf.all.rp_filter=1

sysctl -w net.ipv4.conf.default.rp_filter=1

sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default\.rp_filter[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.rp_filter[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk
 '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.3.7 Ensure Reverse Path Filtering is enabled - net.ipv4.conf.all.rp_filter = 1

Info

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

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.conf.all.rp_filter=1

sysctl -w net.ipv4.conf.default.rp_filter=1

sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.conf.all.rp_filter expect: ^[\s]*net\.ipv4\.conf\.all\.rp_filter[\s]*=[\s]*1[\s]*$
system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.conf.all.rp_filter' returned :

net.ipv4.conf.all.rp_filter = 0
```

3.3.7 Ensure Reverse Path Filtering is enabled - net.ipv4.conf.default.rp_filter = 1

Info

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

Rationale:

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

Solution

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

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

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.conf.all.rp_filter=1

sysctl -w net.ipv4.conf.default.rp_filter=1

sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.conf.default.rp_filter expect: ^[\s]*net\.ipv4\.conf\.default
\.rp_filter[\s]*=[\s]*1[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.conf.default.rp_filter' returned :

net.ipv4.conf.default.rp_filter = 0
```

3.3.8 Ensure TCP SYN Cookies is enabled - files net.ipv4.tcp_syncookies = 1

Info

When tcp_syncookies is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

Rationale:

Attackers use SYN flood attacks to perform a denial of service attacked on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Solution

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

net.ipv4.tcp_syncookies = 1

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.tcp_syncookies=1

sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv4\.tcp_syncookies[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net
\.ipv4\.tcp_syncookies[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.3.9 Ensure IPv6 router advertisements are not accepted - files net.ipv6.conf.all.accept_ra = 0

Info

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

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Solution

IF IPv6 is enabled:

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.all\.accept_ra[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* |/usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.all
\.accept_ra[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* |/usr/bin/awk
 '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.3.9 Ensure IPv6 router advertisements are not accepted - files net.ipv6.conf.default.accept_ra = 0

Info

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

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Solution

IF IPv6 is enabled:

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.default\.accept_ra[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* |/usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.default
\.accept_ra[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* |/usr/bin/awk
 '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.3.9 Ensure IPv6 router advertisements are not accepted - net.ipv6.conf.all.accept_ra = 0

Info

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

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Solution

IF IPv6 is enabled:

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv6.conf.all.accept_ra expect: ^[\s]*net\.ipv6\.conf\.all\.accept_ra[\s]*=[\s]*0[\s]*$
system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv6.conf.all.accept_ra' returned :

net.ipv6.conf.all.accept_ra = 1
```

3.3.9 Ensure IPv6 router advertisements are not accepted - net.ipv6.conf.default.accept_ra = 0

Info

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

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Solution

IF IPv6 is enabled:

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

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

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv6.conf.default.accept_ra expect: ^[\s]*net\.ipv6\.conf\.default \.accept_ra[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv6.conf.default.accept_ra' returned :

net.ipv6.conf.default.accept_ra = 1
```

3.5.3.2 Ensure a table exists

Info

Tables hold chains. Each table only has one address family and only applies to packets of this family. Tables can have one of five families.

Rationale:

nftables doesn't have any default tables. Without a table being build, nftables will not filter network traffic.

Solution

Run the following command to create a table in nftables

nft create table inet <table name>

Example:

nft create table inet filter

Impact:

Adding rules to a running nftables can cause loss of connectivity to the system

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d

NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/nft list tables expect: ^table[\s]+inet[\s]+ system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/nft list tables' did not return any result
```

3.5.3.3 Ensure base chains exist - forward

Info

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

Rationale:

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

Solution

Run the following command to create the base chains:

nft create chain inet <table name> <base chain name> { type filter hook <(input|forward|output)> priority 0 ; }

Example:

nft create chain inet filter input { type filter hook input priority 0 ; }

nft create chain inet filter forward { type filter hook forward priority 0 ; }

nft create chain inet filter output { type filter hook output priority 0 ; }

Impact:

if configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b

HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/nft list ruleset | /bin/grep 'hook forward'

expect: ^type[\s]+filter[\s]+hook[\s]+forward[\s]+priority[\s]+0;

system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/nft list ruleset | /bin/grep 'hook forward'' did not return any result
```

3.5.3.3 Ensure base chains exist - input

Info

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

Rationale:

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

Solution

Run the following command to create the base chains:

nft create chain inet <table name> <base chain name> { type filter hook <(input|forward|output)> priority 0 ; }

Example:

nft create chain inet filter input { type filter hook input priority 0 ; }

nft create chain inet filter forward { type filter hook forward priority 0 ; }

nft create chain inet filter output { type filter hook output priority 0 ; }

Impact:

if configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b

HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/nft list ruleset | /bin/grep 'hook input'

expect: ^type[\s]+filter[\s]+hook[\s]+input[\s]+priority[\s]+0;

system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/nft list ruleset | /bin/grep 'hook input'' did not return any result
```

3.5.3.3 Ensure base chains exist - output

Info

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

Rationale:

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

Solution

Run the following command to create the base chains:

nft create chain inet <table name> <base chain name> { type filter hook <(input|forward|output)> priority 0 ; }

Example:

nft create chain inet filter input { type filter hook input priority 0 ; }

nft create chain inet filter forward { type filter hook forward priority 0 ; }

nft create chain inet filter output { type filter hook output priority 0 ; }

Impact:

if configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b

HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/nft list ruleset | /bin/grep 'hook output'

expect: ^type[\s]+filter[\s]+hook[\s]+output[\s]+priority[\s]+0;

system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/nft list ruleset | /bin/grep 'hook output'' did not return any result
```

3.5.3.4 Ensure loopback traffic is configured - lo

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

nft add rule inet filter input iif lo accept

nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop

IF IPv6 is enabled on the system, run the following command to implement the IPv6 loopback rule:

nft add rule inet filter input ip6 saddr ::1 counter drop

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d

NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/nft list ruleset | /usr/bin/awk '/hook input/,/}/' | /bin/grep 'iif "lo" accept'

expect: iif "lo" accept system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/nft list ruleset | /usr/bin/awk '/hook input/,/}/' | /bin/grep 'iif "lo"
 accept'' did not return any result
```

3.5.3.4 Ensure loopback traffic is configured - v4

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

nft add rule inet filter input iif lo accept

nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop

IF IPv6 is enabled on the system, run the following command to implement the IPv6 loopback rule:

nft add rule inet filter input ip6 saddr ::1 counter drop

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d

NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/nft list ruleset | /usr/bin/awk '/hook input/,/}/' | /bin/grep 'ip saddr'

expect: ip saddr 127.0.0.0/8 counter system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/nft list ruleset | /usr/bin/awk '/hook input/,/}/' | /bin/grep 'ip saddr''
 did not return any result
```

3.5.3.4 Ensure loopback traffic is configured - v6

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

nft add rule inet filter input iif lo accept

nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop

IF IPv6 is enabled on the system, run the following command to implement the IPv6 loopback rule:

nft add rule inet filter input ip6 saddr ::1 counter drop

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d

NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/nft list ruleset | /usr/bin/awk '/hook input/,/}/' | /bin/grep 'ip6 saddr'

expect: ip6 saddr ::1 counter system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/nft list ruleset | /usr/bin/awk '/hook input/,/}/' | /bin/grep 'ip6 saddr''
 did not return any result
```

3.5.3.6 Ensure default deny firewall policy - forward

Info

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

Rationale:

There are two policies: accept (Default) and drop. If the policy is set to accept, the firewall will accept any packet that is not configured to be denied and the packet will continue transversing the network stack.

It is easier to white list acceptable usage than to black list unacceptable usage.

Solution

Run the following command for the base chains with the input, forward, and output hooks to implement a default DROP policy:

nft chain <table family> <table name> <chain name> { policy drop ; }

Example:

nft chain inet filter input { policy drop ; }

nft chain inet filter forward { policy drop ; }

nft chain inet filter output { policy drop ; }

Impact:

if configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

Default Value:

accept

References:

Manual Page nft

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1

800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/nft list ruleset | /bin/grep 'hook forward'

expect: type[\s]+filter[\s]+hook[\s]+forward[\s]+priority[\s]+0;[\s]+policy[\s]+drop;

system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/nft list ruleset | /bin/grep 'hook forward'' did not return any result
```

3.5.3.6 Ensure default deny firewall policy - input

Info

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

Rationale:

There are two policies: accept (Default) and drop. If the policy is set to accept, the firewall will accept any packet that is not configured to be denied and the packet will continue transversing the network stack.

It is easier to white list acceptable usage than to black list unacceptable usage.

Solution

Run the following command for the base chains with the input, forward, and output hooks to implement a default DROP policy:

nft chain <table family> <table name> <chain name> { policy drop ; }

Example:

nft chain inet filter input { policy drop ; }

nft chain inet filter forward { policy drop ; }

nft chain inet filter output { policy drop ; }

Impact:

if configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

Default Value:

accept

References:

Manual Page nft

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1

800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/nft list ruleset | /bin/grep 'hook input'

expect: type[\s]+filter[\s]+hook[\s]+input[\s]+priority[\s]+0;[\s]+policy[\s]+drop;

system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/nft list ruleset | /bin/grep 'hook input'' did not return any result
```

3.5.3.6 Ensure default deny firewall policy - output

Info

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

Rationale:

There are two policies: accept (Default) and drop. If the policy is set to accept, the firewall will accept any packet that is not configured to be denied and the packet will continue transversing the network stack.

It is easier to white list acceptable usage than to black list unacceptable usage.

Solution

Run the following command for the base chains with the input, forward, and output hooks to implement a default DROP policy:

nft chain <table family> <table name> <chain name> { policy drop ; }

Example:

nft chain inet filter input { policy drop ; }

nft chain inet filter forward { policy drop ; }

nft chain inet filter output { policy drop ; }

Impact:

if configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

Default Value:

accept

References:

Manual Page nft

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1

800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/nft list ruleset | /bin/grep 'hook output'

expect: type[\s]+filter[\s]+hook[\s]+output[\s]+priority[\s]+0;[\s]+policy[\s]+drop;

system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/nft list ruleset | /bin/grep 'hook output'' did not return any result
```

3.5.3.7 Ensure nftables service is enabled

Info

The nftables service allows for the loading of nftables rulesets during boot, or starting on the nftables service

Rationale:

The nftables service restores the nftables rules from the rules files referenced in the /etc/nftables.conf file durring boot or the starting of the nftables service

Solution

Run the following command to enable the nftables service:

systemctl enable nftables

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV6	9.1
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1

QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/systemctl is-enabled nftables expect: enabled system: Linux

Hosts

192.168.56.115

```
The command '/bin/systemctl is-enabled nftables' returned :

disabled
```

3.5.4.2.1 Ensure IPv6 default deny firewall policy - Chain FORWARD

Info

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

Rationale:

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

Solution

Run the following commands to implement a default DROP policy:

ip6tables -P INPUT DROP # ip6tables -P OUTPUT DROP # ip6tables -P FORWARD DROP

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26

PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/ip6tables --list | /bin/grep 'Chain FORWARD'

expect: ^Chain FORWARD \(policy DROP\) system: Linux

Hosts

192.168.56.115

```
The command '/sbin/ip6tables --list | /bin/grep 'Chain FORWARD'' returned :

bash: line 1: /sbin/ip6tables: No such file or directory
```

3.5.4.2.1 Ensure IPv6 default deny firewall policy - Chain INPUT

Info

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

Rationale:

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

Solution

Run the following commands to implement a default DROP policy:

ip6tables -P INPUT DROP # ip6tables -P OUTPUT DROP # ip6tables -P FORWARD DROP

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26

PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/ip6tables --list | /bin/grep 'Chain INPUT'

expect: ^Chain INPUT \(policy DROP\) system: Linux

Hosts

192.168.56.115

```
The command '/sbin/ip6tables --list | /bin/grep 'Chain INPUT'' returned :

bash: line 1: /sbin/ip6tables: No such file or directory
```

3.5.4.2.1 Ensure IPv6 default deny firewall policy - Chain OUTPUT

Info

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

Rationale:

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

Solution

Run the following commands to implement a default DROP policy:

ip6tables -P INPUT DROP # ip6tables -P OUTPUT DROP # ip6tables -P FORWARD DROP

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26

PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/ip6tables --list | /bin/grep 'Chain OUTPUT'

expect: ^Chain OUTPUT \(policy DROP\) system: Linux

Hosts

192.168.56.115

```
The command '/sbin/ip6tables --list | /bin/grep 'Chain OUTPUT'' returned :

bash: line 1: /sbin/ip6tables: No such file or directory
```

3.5.4.2.2 Ensure IPv6 loopback traffic is configured - INPUT

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

ip6tables -A INPUT -i lo -j ACCEPT # ip6tables -A OUTPUT -o lo -j ACCEPT # ip6tables -A INPUT -s ::1 -j DROP

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4

NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/ip6tables -L INPUT -v -n | /usr/bin/awk '{ a[$3":"$4":"$5":"$6":"$7":"$8] = NR; print } END { if (a["ACCEPT:all:lo:*:::/0:::/0"] > 0 && a["ACCEPT:all:lo:*:::/0:::/0"] < a["DROP:all:*:*:::1:::/0"]) { print "pass" } else { print "fail" } }'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/ip6tables -L INPUT -v -n | /usr/bin/awk '{ a[$3":"$4":"$5":"$6":"$7":"$8]
 = NR; print } END { if (a["ACCEPT:all:lo:*:::/0:::/0"] > 0 && a["ACCEPT:all:lo:*:::/0:::/0"] <
 a["DROP:all:*:*:::1:::/0"]) { print "pass" } else { print "fail" } }'' returned :

bash: line 1: /usr/sbin/ip6tables: No such file or directory
fail
```

3.5.4.2.2 Ensure IPv6 loopback traffic is configured - OUTPUT

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

ip6tables -A INPUT -i lo -j ACCEPT # ip6tables -A OUTPUT -o lo -j ACCEPT # ip6tables -A INPUT -s ::1 -j DROP

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4

NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/ip6tables -L OUTPUT -v -n | /usr/bin/awk '{ a[$3":"$4":"$5":"$6":"$7":"$8] = NR; print } END { if (a["ACCEPT:all:*:lo:::/0:::/0"] > 0) { print "pass" } else { print "fail" } }'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/ip6tables -L OUTPUT -v -n | /usr/bin/awk '{ a[$3":"$4":"$5":"$6":"$7":"$8]
 = NR; print } END { if (a["ACCEPT:all:*:lo:::/0:::/0"] > 0) { print "pass" } else { print
 "fail" } }'' returned :

bash: line 1: /usr/sbin/ip6tables: No such file or directory
fail
```

4.2.2.1 Ensure journald is configured to send logs to rsyslog

Info

Data from journald may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of journald logs, however, use of the rsyslog service provides a consistent means of log collection and export.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Solution

Edit the /etc/systemd/journald.conf file and add the following line:

ForwardToSyslog=yes

References:

https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf

Notes:

This recommendation assumes that recommendation 4.2.1.5, 'Ensure rsyslog is configured to send logs to a remote log host' has been implemented.

As noted in the journald man pages, journald logs may be exported to rsyslog either through the process mentioned here, or through a facility like systemd-journald.service. There are trade-offs involved in each implementation, where ForwardToSyslog will immediately capture all events (and forward to an external log server, if properly configured), but may not capture all boot-up activities. Mechanisms such as systemd-journald.service, on the other hand, will record bootup events, but may delay sending the information to rsyslog, leading to the potential for log manipulation prior to export. Be aware of the limitations of all tools employed to secure a system.

The main configuration file /etc/systemd/journald.conf is read before any of the custom *.conf files. If there are custom configs present, they override the main configuration parameters

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.8
800-53	AU-9(2)
800-53R5	AU-9(2)
CN-L3	8.1.3.5(d)
CN-L3	8.1.4.3(c)
CSCV7	6.5
CSF	PR.PT-1

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO/IEC-27001	A.12.4.2
ITSG-33	AU-9(2)
LEVEL	1S
NESA	M5.2.3
NESA	M5.5.2
NIAV2	SS13e
PCI-DSSV3.2.1	10.5.3
PCI-DSSV3.2.1	10.5.4
PCI-DSSV4.0	10.3.3
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*ForwardToSyslog[\s]*=[\s]*['"]?yes['"]?[\s]*$ file: /etc/systemd/journald.conf regex: ^[\s]*ForwardToSyslog[\s]*= system: Linux

Hosts

192.168.56.115

```
The file "/etc/systemd/journald.conf" does not contain "^[\s]*ForwardToSyslog[\s]*="
```

4.2.2.2 Ensure journald is configured to compress large log files

Info

The journald system includes the capability of compressing overly large files to avoid filling up the system with logs or making the logs unmanageably large.

Rationale:

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

Solution

Edit the /etc/systemd/journald.conf file and add the following line:

Compress=yes

References:

https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf

Notes:

The main configuration file /etc/systemd/journald.conf is read before any of the custom *.conf files. If there are custom configs present, they override the main configuration parameters

See Also

https://workbench.cisecurity.org/files/2658

References

800-53	AU-4
800-53R5	AU-4
CSCV7	6.4
CSF	PR.DS-4
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-4
LEVEL	1S
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*Compress[\s]*=[\s]*yes[\s]*$ file: /etc/systemd/journald.conf regex: ^[\s]*Compress[\s]*= system: Linux

Hosts

192.168.56.115

```
The file "/etc/systemd/journald.conf" does not contain "^[\s]*Compress[\s]*="
```

4.2.2.3 Ensure journald is configured to write logfiles to persistent disk

Info

Data from journald may be stored in volatile memory or persisted locally on the server. Logs in memory will be lost upon a system reboot. By persisting logs to local disk on the server they are protected from loss.

Rationale:

Writing log data to disk will provide the ability to forensically reconstruct events which may have impacted the operations or security of a system even after a system crash or reboot.

Solution

Edit the /etc/systemd/journald.conf file and add the following line:

Storage=persistent

References:

https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf

Notes:

The main configuration file /etc/systemd/journald.conf is read before any of the custom *.conf files. If there are custom configs present, they override the main configuration parameters

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*Storage[\s]*=[\s]*persistent[\s]*$ file: /etc/systemd/journald.conf regex: ^[\s]*Storage[\s]*= system: Linux

Hosts

192.168.56.115

```
The file "/etc/systemd/journald.conf" does not contain "^[\s]*Storage[\s]*="
```

4.2.3 Ensure permissions on all logfiles are configured

Info

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

Rationale:

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

Solution

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

find /var/log -type f -exec chmod g-wx,o-rwx '{}' + -o -type d -exec chmod g-w,o-rwx '{}' +

Notes:

You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(10)
800-53R5	SC-7(10)
CN-L3	8.1.10.6(j)
CSCV6	3.1
CSCV7	13
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(10)
LEVEL	1S
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a

NIAV2	GS2b
PCI-DSSV3.2.1	1.1
PCI-DSSV3.2.1	1.2
PCI-DSSV3.2.1	1.2.1
PCI-DSSV3.2.1	1.3
PCI-DSSV4.0	1.3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: OUTPUT=$(ls -l /var/log); /usr/bin/find /var/log -type f -perm /g+wx,o+rwx -ls | /bin/awk -v awkvar="${OUTPUT}" '{print} END {if (NR == 0) print awkvar "

pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command 'OUTPUT=$(ls -l /var/log); /usr/bin/find /var/log -type f -perm /g+wx,o+rwx -ls | /bin/
awk -v awkvar="${OUTPUT}" '{print} END {if (NR == 0) print awkvar "\npass" ; else print "fail"}''
 returned :

656867      8 -rw-r--r--   1 root     root         5463 Jul 26 10:03 /var/log/fontconfig.log
   653058     52 -rw-r--r--   1 root     root        47648 Jul 26 10:05 /var/log/alternatives.log
   652845     60 -rw-r--r--   1 root     root        61226 Jul 26 10:06 /var/log/installer/status
   652843     24 -rw-r--r--   1 root     root        21138 Jul 26 10:06 /var/log/installer/hardware-
summary
   652846      4 -rw-r--r--   1 root     root          162 Jul 26 10:06 /var/log/installer/lsb-
release
   652851      4 -rw-r--r--   1 root     root          117 Jul 26 10:06 /var/log/installer/firmware-
summary
   653002    788 -rw-r--r--   1 root     root       799365 Jul 26 16:46 /var/log/dpkg.log
   653337      0 -rw-r--r--   1 root     root            0 Jul 26 09:40 /var/log/faillog
   653030    176 -rw-rw-r--   1 root     utmp       175488 Aug  1 09:42 /var/log/wtmp
   653031      4 -rw-rw----   1 root     utmp         2304 Aug  1 09:35 /var/log/btmp
   652811     24 -rw-r--r--   1 root     root        20745 Jul 26 10:05 /var/log/vboxpostinstall.log
   653032      4 -rw-rw-r--   1 root     utmp       292292 Aug  1 09:42 /var/log/lastlog
   652814     60 -rw-r--r--   1 root     root        60772 Jul 26 16:46 /var/log/apt/eipp.log.xz
   653379     72 -rw-r--r--   1 root     root        70717 Jul 26 16:46 /var/log/apt/history.log
fail
```

4.4 Ensure logrotate assigns appropriate permissions

Info

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

Rationale:

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

Solution

Edit /etc/logrotate.conf and update the create line to read 0640 or more restrictive, following local site policy Example

create 0640 root utmp

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4

NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: (0)?[0-6][04]0 file: /etc/logrotate.conf /etc/logrotate.d/* min_occurrences: 1 regex: ^[\s]*create[\s]+[\S]+ required: NO system: Linux

Hosts

192.168.56.115

```
Non-compliant file(s):
      /etc/logrotate.d/alternatives - regex '^[\s]*create[\s]+[\S]+' found - expect '(0)?[0-6][04]0'
 not found in the following lines:
          8: create 644 root root
      /etc/logrotate.d/btmp - regex '^[\s]*create[\s]+[\S]+' found - expect '(0)?[0-6][04]0' not
 found in the following lines:
          5:     create 0660 root utmp
      /etc/logrotate.d/dpkg - regex '^[\s]*create[\s]+[\S]+' found - expect '(0)?[0-6][04]0' not
 found in the following lines:
          8: create 644 root root
      /etc/logrotate.d/wtmp - regex '^[\s]*create[\s]+[\S]+' found - expect '(0)?[0-6][04]0' not
 found in the following lines:
          5:     create 0664 root utmp
```

5.1.2 Ensure permissions on /etc/crontab are configured

Info

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

Rationale:

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

Solution

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

chown root:root /etc/crontab

chmod og-rwx /etc/crontab

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S

NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/crontab group: root mask: 177 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/crontab with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 177 uneven
 permissions : FALSE

/etc/crontab
```

5.1.3 Ensure permissions on /etc/cron.hourly are configured

Info

This directory contains system cron jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Solution

Run the following commands to set ownership and permissions on /etc/cron.hourly :

chown root:root /etc/cron.hourly

chmod og-rwx /etc/cron.hourly

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3

LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/cron.hourly group: root mask: 077 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/cron.hourly with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.hourly
```

5.1.4 Ensure permissions on /etc/cron.daily are configured

Info

The /etc/cron.daily directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Solution

Run the following commands to set ownership and permissions on /etc/cron.daily :

chown root:root /etc/cron.daily

chmod og-rwx /etc/cron.daily

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3

LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/cron.daily group: root mask: 077 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/cron.daily with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.daily
```

5.1.5 Ensure permissions on /etc/cron.weekly are configured

Info

The /etc/cron.weekly directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Solution

Run the following commands to set ownership and permissions on /etc/cron.weekly :

chown root:root /etc/cron.weekly

chmod og-rwx /etc/cron.weekly

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3

LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/cron.weekly group: root mask: 077 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/cron.weekly with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.weekly
```

5.1.6 Ensure permissions on /etc/cron.monthly are configured

Info

The /etc/cron.monthly directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Solution

Run the following commands to set ownership and permissions on /etc/cron.monthly :

chown root:root /etc/cron.monthly

chmod og-rwx /etc/cron.monthly

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3

LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/cron.monthly group: root mask: 077 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/cron.monthly with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.monthly
```

5.1.7 Ensure permissions on /etc/cron.d are configured

Info

The /etc/cron.d directory contains system cron jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from /etc/crontab , but require more granular control as to when they run. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Solution

Run the following commands to set ownership and permissions on /etc/cron.d :

chown root:root /etc/cron.d

chmod og-rwx /etc/cron.d

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3

LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/cron.d group: root mask: 077 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/cron.d with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.d
```

5.1.8 Ensure at/cron is restricted to authorized users - at.allow

Info

Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. If /etc/cron.allow or /etc/at.allow do not exist, then /etc/at.deny and /etc/cron.deny are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in /etc/cron.allow and /etc/at.allow are allowed to use at and cron. Note that even though a given user is not listed in cron.allow , cron jobs can still be run as that user. The cron.allow file only controls administrative access to the crontab command for scheduling and modifying cron jobs.

Rationale:

On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Solution

Run the following commands to remove /etc/cron.deny, create /etc/cron.allow, and set permissions and ownership for /etc/cron.allow:

rm /etc/cron.deny # touch /etc/cron.allow # chown root:root /etc/cron.allow # chmod g-wx,o-rwx /etc/cron.allow

If at is installed on the system:

Run the following commands to remove /etc/at.deny; create /etc/at.allow, and set ownership and permissions on/etc/at.allow`:

rm /etc/at.deny # touch /etc/at.allow # chown root:root /etc/at.allow # chmod g-wx,o-rwx /etc/at.allow

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/at.allow group: root mask: 137 owner: root system: Linux

Hosts

192.168.56.115

```
No files found: /etc/at.allow
```

5.1.8 Ensure at/cron is restricted to authorized users - cron.allow

Info

Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. If /etc/cron.allow or /etc/at.allow do not exist, then /etc/at.deny and /etc/cron.deny are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in /etc/cron.allow and /etc/at.allow are allowed to use at and cron. Note that even though a given user is not listed in cron.allow , cron jobs can still be run as that user. The cron.allow file only controls administrative access to the crontab command for scheduling and modifying cron jobs.

Rationale:

On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Solution

Run the following commands to remove /etc/cron.deny, create /etc/cron.allow, and set permissions and ownership for /etc/cron.allow:

rm /etc/cron.deny # touch /etc/cron.allow # chown root:root /etc/cron.allow # chmod g-wx,o-rwx /etc/cron.allow

If at is installed on the system:

Run the following commands to remove /etc/at.deny; create /etc/at.allow, and set ownership and permissions on/etc/at.allow`:

rm /etc/at.deny # touch /etc/at.allow # chown root:root /etc/at.allow # chmod g-wx,o-rwx /etc/at.allow

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/cron.allow group: root mask: 137 owner: root system: Linux

Hosts

192.168.56.115

```
No files found: /etc/cron.allow
```

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

Info

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

Rationale:

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

Solution

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

chown root:root /etc/ssh/sshd_config

chmod og-rwx /etc/ssh/sshd_config

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4

NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/ssh/sshd_config group: root mask: 077 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/ssh/sshd_config with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/ssh/sshd_config
```

5.2.4 Ensure SSH Protocol is not set to 1

Info

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

Rationale:

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

Solution

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

Protocol 2

Notes:

This command not longer exists in newer versions of SSH. This check is still being included for systems that may be running an older version of SSH. As of openSSH version 7.4 this parameter will not cause an issue when included.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.3
800-171	3.13.8
800-53	IA-2(1)
800-53	SC-8
800-53R5	IA-2(1)
800-53R5	SC-8
CN-L3	7.1.2.7(b)
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSCV7	4.5
CSCV7	14.4
CSF	PR.AC-1
CSF	PR.DS-2

CSF	PR.DS-5
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ITSG-33	IA-2(1)
ITSG-33	SC-8
ITSG-33	SC-8a.
LEVEL	1S
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T5.4.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	AM36
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
NIAV2	VL3c
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	1.2
TBA-FIISB	35.1
TBA-FIISB	36.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(?i)Protocol(?-i)[\s]+2[\s]*$ file: /etc/ssh/sshd_config regex: ^[\s]*(?i)Protocol(?-i)[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)Protocol(?-i)[\s]"
```

5.2.5 Ensure SSH LogLevel is appropriate

Info

INFO level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

VERBOSE level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments.

Rationale:

SSH provides several logging levels with varying amounts of verbosity. DEBUG is specifically not recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

Solution

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

LogLevel VERBOSE

OR

LogLevel INFO

Default Value:

LogLevel INFO

References:

https://www.ssh.com/ssh/sshd_config/

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)

CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(?i)LogLevel(?-i)[\s]+(INFO|VERBOSE)[\s]*$ file: /etc/ssh/sshd_config regex: ^[\s]*(?i)LogLevel(?-i)[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)LogLevel(?-i)[\s]"
```

5.2.7 Ensure SSH MaxAuthTries is set to 4 or less

Info

The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure.

Rationale:

Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Solution

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

MaxAuthTries 4

Default Value:

MaxAuthTries 6

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.2
800-53	AC-2(12)
800-53R5	AC-2(12)
CN-L3	7.1.3.2(d)
CSCV6	16.7
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NESA	M5.3.1
NIAV2	AM28

NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(?i)MaxAuthTries(?-i)[\s]+[1-4][\s]*$ file: /etc/ssh/sshd_config regex: ^[\s]*(?i)MaxAuthTries(?-i)[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)MaxAuthTries(?-i)[\s]"
```

5.2.9 Ensure SSH HostbasedAuthentication is disabled

Info

The HostbasedAuthentication parameter specifies if authentication is allowed through trusted hosts via the user of .rhosts, or /etc/hosts.equiv, along with successful public key client host authentication. This option only applies to SSH Protocol Version 2.

Rationale:

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

Solution

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

HostbasedAuthentication no

Default Value:

HostbasedAuthentication no

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	AC-14a.
800-53	IA-5
800-53R5	AC-14a.
800-53R5	IA-5
CSCV7	16.3
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	AC-14a.
ITSG-33	IA-5
LEVEL	1S
NESA	T5.2.3
NESA	T5.6.1
QCSC-V1	5.2.2
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(?i)HostbasedAuthentication(?-i)[\s]+no[\s]*$ file: /etc/ssh/sshd_config regex: ^[\s]*(?i)HostbasedAuthentication(?-i)[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)HostbasedAuthentication(?-i)[\s]"
```

5.2.10 Ensure SSH root login is disabled

Info

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

Rationale:

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

Solution

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

PermitRootLogin no

Default Value:

PermitRootLogin without-password

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2(9)
800-53R5	AC-2(9)
CN-L3	8.1.4.2(c)
CSCV7	4.3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM16
PCI-DSSV3.2.1	8.5
PCI-DSSV4.0	8.2.2
PCI-DSSV4.0	8.2.3
QCSC-V1	5.2.2
QCSC-V1	8.2.1

QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(?i)PermitRootLogin(?-i)[\s]+no[\s]*$ file: /etc/ssh/sshd_config regex: ^[\s]*(?i)PermitRootLogin(?-i)[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)PermitRootLogin(?-i)[\s]"
```

5.2.11 Ensure SSH PermitEmptyPasswords is disabled

Info

The PermitEmptyPasswords parameter specifies if the SSH server allows login to accounts with empty password strings.

Rationale:

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system

Solution

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

PermitEmptyPasswords no

Default Value:

PermitEmptyPasswords no

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5
800-53R5	IA-5
CSCV7	16.3
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(?i)PermitEmptyPasswords(?-i)[\s]+no[\s]*$ file: /etc/ssh/sshd_config regex: ^[\s]*(?i)PermitEmptyPasswords(?-i)[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)PermitEmptyPasswords(?-i)[\s]"
```

5.2.12 Ensure SSH PermitUserEnvironment is disabled

Info

The PermitUserEnvironment option allows users to present environment options to the ssh daemon.

Rationale:

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has ssh executing trojan'd programs)

Solution

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

PermitUserEnvironment no

Default Value:

PermitUserEnvironment no

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(?i)PermitUserEnvironment(?-i)[\s]+no[\s]*$ file: /etc/ssh/sshd_config regex: ^[\s]*(?i)PermitUserEnvironment(?-i)[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)PermitUserEnvironment(?-i)[\s]"
```

5.2.14 Ensure only strong MAC algorithms are used

Info

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

Rationale:

MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Edit the /etc/ssh/sshd_config file and add/modify the MACs line to contain a comma separated list of the site approved MACs Example:

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

Default Value:

MACs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

References:

More information on SSH downgrade attacks can be found here: http://www.mitls.org/pages/attacks/SLOTH

SSHD_CONFIG(5)

Notes:

Some organizations may have stricter requirements for approved MACs. Ensure that MACs used are in compliance with site policy.

The only 'strong' MACs currently FIPS 140-2 approved are hmac-sha2-256 and hmac-sha2-512

The Supported MACs are:

hmac-md5

hmac-md5-96

hmac-ripemd160

hmac-sha1

hmac-sha1-96

hmac-sha2-256

hmac-sha2-512

umac-64@openssh.com

umac-128@openssh.com

hmac-md5-etm@openssh.com

hmac-md5-96-etm@openssh.com

hmac-ripemd160-etm@openssh.com

hmac-sha1-etm@openssh.com

hmac-sha1-96-etm@openssh.com

hmac-sha2-256-etm@openssh.com

hmac-sha2-512-etm@openssh.com

umac-64-etm@openssh.com

umac-128-etm@openssh.com

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-171	3.13.8
800-53	IA-5
800-53	SC-8
800-53R5	IA-5
800-53R5	SC-8
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSCV7	14.4
CSCV7	16.5
CSF	PR.AC-1
CSF	PR.DS-2
CSF	PR.DS-5

GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ITSG-33	IA-5
ITSG-33	SC-8
ITSG-33	SC-8a.
LEVEL	1S
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T5.2.3
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/sshd -T | /bin/grep -i 'MACs' | /bin/grep -oP '((hmac-md5|hmac-md5-96|hmac-ripemd160|hmac-sha1|hmac-sha1-96|hmac-sha1-96|umac-64@openssh.com|umac-128@openssh.com|hmac-md5-etm@openssh.com|hmac-md5-96-etm@openssh.com|hmac-ripemd160-etm@openssh.com|hmac-sha1-etm@openssh.com|hmac-sha1-96-etm@openssh.com|umac-64-etm@openssh.com|umac-128-etm@openssh.com)[,]?)+' | /bin/awk '{print} END {if (NR == 0) print "pass"; else print $0 }'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/sshd -T | /bin/grep -i 'MACs' | /bin/grep -oP '((hmac-md5|hmac-md5-96|
hmac-ripemd160|hmac-sha1|hmac-sha1-96|hmac-sha1-96|umac-64@openssh.com|umac-128@openssh.com|
hmac-md5-etm@openssh.com|hmac-md5-96-etm@openssh.com|hmac-ripemd160-etm@openssh.com|hmac-sha1-
etm@openssh.com|hmac-sha1-96-etm@openssh.com|umac-64-etm@openssh.com|umac-128-etm@openssh.com)
[,]?)+' | /bin/awk '{print} END {if (NR == 0) print "pass"; else print $0 }'' returned :

umac-64-etm@openssh.com,umac-128-etm@openssh.com,
hmac-sha1
umac-64@openssh.com,umac-128@openssh.com,
hmac-sha1
hmac-sha1
```

5.2.16 Ensure SSH Idle Timeout Interval is configured - ClientAliveInterval

Info

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

Rationale:

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

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

Solution

Edit the /etc/ssh/sshd_config file to set the parameters according to site policy:

ClientAliveInterval 300

ClientAliveCountMax 0

Default Value:

ClientAliveInterval 300

ClientAliveCountMax 0

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.10
800-53	AC-11
800-53R5	AC-11
CN-L3	8.1.4.1(b)
CSCV7	16.11
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO/IEC-27001	A.11.2.8

ITSG-33	AC-11
LEVEL	1S
NIAV2	AM23c
NIAV2	AM23d
PCI-DSSV3.2.1	8.1.8
PCI-DSSV4.0	8.2.8

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/sshd -T | /bin/grep clientaliveinterval expect: ^[\s]*clientaliveinterval[\s]+([1-9]|[1-8][0-9]|9[0-9]|[12][0-9]{2}|300)[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/sshd -T | /bin/grep clientaliveinterval' returned :

clientaliveinterval 0
```

5.2.17 Ensure SSH LoginGraceTime is set to one minute or less

Info

The LoginGraceTime parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access.

Rationale:

Setting the LoginGraceTime parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

Solution

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

LoginGraceTime 60

Default Value:

LoginGraceTime 120

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/sshd -T | /bin/grep logingracetime expect: ^[\s]*logingracetime[\s]+([1-9]|[1-5][0-9]|60)[\s]* $ system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/sshd -T | /bin/grep logingracetime' returned :

logingracetime 120
```

5.2.18 Ensure SSH access is limited

Info

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

AllowUsers

The AllowUsers variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.

AllowGroups

The AllowGroups variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

DenyUsers

The DenyUsers variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.

DenyGroups

The DenyGroups variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

Rationale:

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Solution

Edit the /etc/ssh/sshd_config file to set one or more of the parameter as follows:

AllowUsers <userlist>

AllowGroups <grouplist>

DenyUsers <userlist>

DenyGroups <grouplist>

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2(9)
800-53R5	AC-2(9)
CN-L3	8.1.4.2(c)
CSCV7	4.3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM16
PCI-DSSV3.2.1	8.5
PCI-DSSV4.0	8.2.2
PCI-DSSV4.0	8.2.3
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(?i)(Allow|Deny)(Users|Groups)(?-i)[\s] file: /etc/ssh/sshd_config regex: ^[\s]*(?i)(Allow|Deny)(Users|Groups)(?-i)[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)(Allow|Deny)(Users|Groups)(?-i)[\s]"
```

5.2.19 Ensure SSH warning banner is configured

Info

The Banner parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

Rationale:

Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

Solution

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

Banner /etc/issue.net

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(?i)Banner(?-i)[\s]+/etc/issue\.net[\s]*$ file: /etc/ssh/sshd_config regex: ^[\s]*(?i)Banner(?-i)[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)Banner(?-i)[\s]"
```

5.2.22 Ensure SSH MaxStartups is configured

Info

The MaxStartups parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.

Rationale:

To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of MaxStartups to protect availability of sshd logins and prevent overwhelming the daemon.

Solution

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

maxstartups 10:30:60

Notes:

Local site policy may be more restrictive

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(?i)MaxStartups(?-i)[\s]+10:30:60[\s]*$ file: /etc/ssh/sshd_config regex: ^[\s]*(?i)MaxStartups(?-i)[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)MaxStartups(?-i)[\s]"
```

5.3.1 Ensure password creation requirements are configured - minlen

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more. The following are definitions of the pam_pwquality.so options.

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

Password Length:

minlen = 14 - password must be 14 characters or more

Password complexity:

minclass = 4 - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

OR

dcredit = -1 - provide at least one digit

ucredit = -1 - provide at least one uppercase character

ocredit = -1 - provide at least one special character

lcredit = -1 - provide at least one lowercase character

The following is st in the /etc/pam.d/common-password file

retry=3 - Allow 3 tries before sending back a failure.

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

Rationale:

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

Solution

Run the following command to install the pam_pwquality module:

apt install libpam-pwquality

Edit the file /etc/security/pwquality.conf and add or modify the following line for password length to conform to site policy

minlen = 14

Edit the file /etc/security/pwquality.conf and add or modify the following line for password complexity to conform to site policy

minclass = 4

OR

dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1

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

password requisite pam_pwquality.so retry=3

Notes:

Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.

Settings in /etc/security/pwquality.conf must use spaces around the = symbol.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*minlen[\s]*=[\s]*(1[4-9]|[2-9][0-9])[\s]*$ file: /etc/security/pwquality.conf regex: ^[\s]*minlen[\s]*= system: Linux

Hosts

192.168.56.115

```
The file "/etc/security/pwquality.conf" does not contain "^[\s]*minlen[\s]*="
```

5.3.1 Ensure password creation requirements are configured - password complexity

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more. The following are definitions of the pam_pwquality.so options.

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

Password Length:

minlen = 14 - password must be 14 characters or more

Password complexity:

minclass = 4 - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

OR

dcredit = -1 - provide at least one digit

ucredit = -1 - provide at least one uppercase character

ocredit = -1 - provide at least one special character

lcredit = -1 - provide at least one lowercase character

The following is st in the /etc/pam.d/common-password file

retry=3 - Allow 3 tries before sending back a failure.

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

Rationale:

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

Solution

Run the following command to install the pam_pwquality module:

apt install libpam-pwquality

Edit the file /etc/security/pwquality.conf and add or modify the following line for password length to conform to site policy

minlen = 14

Edit the file /etc/security/pwquality.conf and add or modify the following line for password complexity to conform to site policy

minclass = 4

OR

dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1

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

password requisite pam_pwquality.so retry=3

Notes:

Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.

Settings in /etc/security/pwquality.conf must use spaces around the = symbol.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/grep -P '^[[:space:]]*\Scredit[[:space:]]*=[[:space:]]*-[1-9]' /etc/security/pwquality.conf | /usr/bin/sed ':a;$!{N;s/ / /;ba;}' | /usr/bin/grep -P '(?=.*?dcredit).*(?=.*?ucredit).*(?=.*?ocredit).*(?=.*?lcredit)' | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/grep -P '^[[:space:]]*\Scredit[[:space:]]*=[[:space:]]*-[1-9]' /etc/security/
pwquality.conf | /usr/bin/sed ':a;$!{N;s/\n/ /;ba;}' | /usr/bin/grep -P '(?=.*?dcredit).*(?=.*?
ucredit).*(?=.*?ocredit).*(?=.*?lcredit)' | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ;
 else print "fail"}'' returned :

fail
```

5.3.1 Ensure password creation requirements are configured - retry=3

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more. The following are definitions of the pam_pwquality.so options.

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

Password Length:

minlen = 14 - password must be 14 characters or more

Password complexity:

minclass = 4 - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

OR

dcredit = -1 - provide at least one digit

ucredit = -1 - provide at least one uppercase character

ocredit = -1 - provide at least one special character

lcredit = -1 - provide at least one lowercase character

The following is st in the /etc/pam.d/common-password file

retry=3 - Allow 3 tries before sending back a failure.

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

Rationale:

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

Solution

Run the following command to install the pam_pwquality module:

apt install libpam-pwquality

Edit the file /etc/security/pwquality.conf and add or modify the following line for password length to conform to site policy

minlen = 14

Edit the file /etc/security/pwquality.conf and add or modify the following line for password complexity to conform to site policy

minclass = 4

OR

dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1

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

password requisite pam_pwquality.so retry=3

Notes:

Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.

Settings in /etc/security/pwquality.conf must use spaces around the = symbol.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV6	16.7
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: [\s]+retry[\s]*=[\s]*[1-3] file: /etc/pam.d/common-password regex: ^[\s]*password[\s]+requisite[\s]+pam_pwquality\.so[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/pam.d/common-password" does not contain
 "^[\s]*password[\s]+requisite[\s]+pam_pwquality\.so[\s]"
```

5.3.2 Ensure lockout for failed password attempts is configured - /etc/pam.d/common-auth

Info

Lock out users after n unsuccessful consecutive login attempts. The first sets of changes are made to the PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM.

deny=n - n represents the number of failed attempts before the account is locked

unlock_time=n - n represents the number of seconds before the account is unlocked

audit - Will log the user name into the system log if the user is not found.

silent - Don't print informative messages.

Set the lockout number and unlock time in accordance with local site policy.

Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Solution

Edit the /etc/pam.d/common-auth file and add the auth line below:

auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900

Edit the /etc/pam.d/common-account file and add the account lines bellow:

account requisite pam_deny.so account required pam_tally2.so

Note: If a user has been locked out because they have reached the maximum consecutive failure count defined by deny= in the pam_tally2.so module, the user can be unlocked by issuing the command /sbin/pam_tally2 -u <username> --reset. This command sets the failed count to 0, effectively unlocking the user.

Notes:

BUG In pam_tally2.so

To work around this issue you have to add pam_tally2 to the account section account required pam_tally2.so for the counter to reset to 0 when using sudo

Use of the 'audit' keyword may log credentials in the case of user error during authentication. This risk should be evaluated in the context of the site policies of your organization.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2
800-53R5	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16.7
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -P '^[\s]*auth[\s]+required[\s]+pam_tally2\.so[\s]*' /etc/pam.d/common-auth | /bin/grep -P '(?=.*?onerr=fail).*(?=.*?audit).*(?=.*?silent).*(?=.*?deny=5).*(?=.*?unlock_time=900)' | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -P '^[\s]*auth[\s]+required[\s]+pam_tally2\.so[\s]*' /etc/pam.d/common-
auth | /bin/grep -P '(?=.*?onerr=fail).*(?=.*?audit).*(?=.*?silent).*(?=.*?deny=5).*(?=.*?
unlock_time=900)' | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}''
 returned :

fail
```

5.3.2 Ensure lockout for failed password attempts is configured - pam_tally2.so

Info

Lock out users after n unsuccessful consecutive login attempts. The first sets of changes are made to the PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM.

deny=n - n represents the number of failed attempts before the account is locked

unlock_time=n - n represents the number of seconds before the account is unlocked

audit - Will log the user name into the system log if the user is not found.

silent - Don't print informative messages.

Set the lockout number and unlock time in accordance with local site policy.

Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Solution

Edit the /etc/pam.d/common-auth file and add the auth line below:

auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900

Edit the /etc/pam.d/common-account file and add the account lines bellow:

account requisite pam_deny.so account required pam_tally2.so

Note: If a user has been locked out because they have reached the maximum consecutive failure count defined by deny= in the pam_tally2.so module, the user can be unlocked by issuing the command /sbin/pam_tally2 -u <username> --reset. This command sets the failed count to 0, effectively unlocking the user.

Notes:

BUG In pam_tally2.so

To work around this issue you have to add pam_tally2 to the account section account required pam_tally2.so for the counter to reset to 0 when using sudo

Use of the 'audit' keyword may log credentials in the case of user error during authentication. This risk should be evaluated in the context of the site policies of your organization.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2
800-53R5	AC-2
CN-L3	7.1.3.2(d)
CSCV6	16.7
CSCV7	16.7
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*account[\s]+required[\s]+pam_tally2\.so[\s]*$ file: /etc/pam.d/common-account regex: ^[\s]*account[\s]+required[\s]+pam_tally2\.so[\s]* system: Linux

Hosts

192.168.56.115

```
The file "/etc/pam.d/common-account" does not contain
 "^[\s]*account[\s]+required[\s]+pam_tally2\.so[\s]*"
```

5.3.3 Ensure password reuse is limited

Info

The /etc/security/opasswd file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

Rationale:

Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password.

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

Solution

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

password required pam_pwhistory.so remember=5

Notes:

Additional module options may be set, recommendation only covers those listed here.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2
800-53R5	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j

NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: remember=([5-9]|1[0-9]|[2-9][0-9]) file: /etc/pam.d/common-password regex: ^[\s]*password[\s]*required[\s]*pam_pwhistory\.so system: Linux

Hosts

192.168.56.115

```
The file "/etc/pam.d/common-password" does not contain
 "^[\s]*password[\s]*required[\s]*pam_pwhistory\.so"
```

5.3.4 Ensure password hashing algorithm is SHA-512

Info

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

Rationale:

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

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

Solution

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

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

Notes:

Consult your documentation for the appropriate PAM file and module.

Additional module options may be set, recommendation only covers those listed here.

If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login. To accomplish that, the following commands can be used. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

awk -F: '($3 >= $(awk '/^s*UID_MIN/{print $2}' /etc/login.defs) && $1 != 'nfsnobody') { print $1 }' /etc/passwd | xargs -n 1 chage -d 0

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
800-53R5	IA-5
800-53R5	IA-5(1)
CSCV7	16.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^password.*pam_unix.so.*sha512$ file: /etc/pam.d/common-password regex: ^password.*pam_unix.so.*sha512$ system: Linux

Hosts

192.168.56.115

```
The file "/etc/pam.d/common-password" does not contain "^password.*pam_unix.so.*sha512$"
```

5.4.1.1 Ensure password expiration is 365 days or less - login.defs

Info

The PASS_MAX_DAYS parameter in /etc/login.defs allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the PASS_MAX_DAYS parameter be set to less than or equal to 365 days.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Solution

Set the PASS_MAX_DAYS parameter to conform to site policy in /etc/login.defs :

PASS_MAX_DAYS 365

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

chage --maxdays 365 <user>

Notes:

You can also check this setting in /etc/shadow directly. The 5th field should be 365 or less for all users with a password.

Note: A value of -1 will disable password expiration. Additionally the password expiration must be greater than the minimum days between password changes or users will be unable to change their password.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3

QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*PASS_MAX_DAYS[\s]+([1-9]|[1-8][0-9]|9[0-9]|[12][0-9]{2}|3[0-5][0-9]|36[0-5])[\s]*$ file: /etc/login.defs regex: ^[\s]*PASS_MAX_DAYS[\s] system: Linux

Hosts

192.168.56.115

```
Non-compliant file(s):
      /etc/login.defs - regex '^[\s]*PASS_MAX_DAYS[\s]' found - expect
 '^[\s]*PASS_MAX_DAYS[\s]+([1-9]|[1-8][0-9]|9[0-9]|[12][0-9]{2}|3[0-5][0-9]|36[0-5])[\s]*$' not
 found in the following lines:
         165: PASS_MAX_DAYS99999
```

5.4.1.1 Ensure password expiration is 365 days or less - users

Info

The PASS_MAX_DAYS parameter in /etc/login.defs allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the PASS_MAX_DAYS parameter be set to less than or equal to 365 days.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Solution

Set the PASS_MAX_DAYS parameter to conform to site policy in /etc/login.defs :

PASS_MAX_DAYS 365

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

chage --maxdays 365 <user>

Notes:

You can also check this setting in /etc/shadow directly. The 5th field should be 365 or less for all users with a password.

Note: A value of -1 will disable password expiration. Additionally the password expiration must be greater than the minimum days between password changes or users will be unable to change their password.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3

QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^([^:]*:){4}([1-9]|[1-8][0-9]|9[0-9]|[12][0-9]{2}|3[0-5][0-9]|36[0-5]):
file: /etc/shadow regex: ^[^:]+:[^!*] system: Linux

Hosts

192.168.56.115

```
Non-compliant file(s):
      /etc/shadow - regex '^[^:]+:[^!*]' found - expect '^([^:]*:){4}([1-9]|[1-8][0-9]|9[0-9]|[12]
[0-9]{2}|3[0-5][0-9]|36[0-5]):' not found in the following lines:
          1: root:$y$j9T$ZAqGpmZL3dXmFzpLMRTKx0$x7nVBwwUPiI4A595o/
jLRCAUWT10oiGJdT3OnMFV04.:19570:0:99999:7:::
          36: vboxuser:$y$j9T$O5FXW0Or0OEDOaH5WFYR/0$XG7pxQmdZn.DNX/nilAfUUvOCJnLnD3t4fHRe1/
Z/53:19564:0:99999:7:::
```

5.4.1.2 Ensure minimum days between password changes is configured - login.defs

Info

The PASS_MIN_DAYS parameter in /etc/login.defs allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that PASS_MIN_DAYS parameter be set to 1 or more days.

Rationale:

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Solution

Set the PASS_MIN_DAYS parameter to 1 in /etc/login.defs :

PASS_MIN_DAYS 1

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

chage --mindays 1 <user>

Notes:

You can also check this setting in /etc/shadow directly. The 4th field should be 1 or more for all users with a password.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV6	16
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2

QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: PASS_MIN_DAYS[\s]+(?:[1-9]|[1-9][0-9]+)(?:[\s]*|[\s]+\#?.*)$ file: /etc/login.defs regex: ^[\s\t]*PASS_MIN_DAYS[\s]+ system: Linux

Hosts

192.168.56.115

```
Non-compliant file(s):
      /etc/login.defs - regex '^[\s\t]*PASS_MIN_DAYS[\s]+' found - expect 'PASS_MIN_DAYS[\s]+(?:
[1-9]|[1-9][0-9]+)(?:[\s]*|[\s]+\#?.*)$' not found in the following lines:
          166: PASS_MIN_DAYS0
```

5.4.1.2 Ensure minimum days between password changes is configured - users

Info

The PASS_MIN_DAYS parameter in /etc/login.defs allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that PASS_MIN_DAYS parameter be set to 1 or more days.

Rationale:

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Solution

Set the PASS_MIN_DAYS parameter to 1 in /etc/login.defs :

PASS_MIN_DAYS 1

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

chage --mindays 1 <user>

Notes:

You can also check this setting in /etc/shadow directly. The 4th field should be 1 or more for all users with a password.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV6	16
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2

SWIFT-CSCV1 4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^([^:]*:){3}(?:[1-9]|[1-9][0-9]+):

file: /etc/shadow regex: ^[^:]+:[^!*] system: Linux

Hosts

192.168.56.115

```
Non-compliant file(s):
      /etc/shadow - regex '^[^:]+:[^!*]' found - expect '^([^:]*:){3}(?:[1-9]|[1-9][0-9]+):' not
 found in the following lines:
          1: root:$y$j9T$ZAqGpmZL3dXmFzpLMRTKx0$x7nVBwwUPiI4A595o/
jLRCAUWT10oiGJdT3OnMFV04.:19570:0:99999:7:::
          36: vboxuser:$y$j9T$O5FXW0Or0OEDOaH5WFYR/0$XG7pxQmdZn.DNX/nilAfUUvOCJnLnD3t4fHRe1/
Z/53:19564:0:99999:7:::
```

5.4.1.4 Ensure inactive password lock is 30 days or less - useradd

Info

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Solution

Run the following command to set the default password inactivity period to 30 days:

useradd -D -f 30

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

chage --inactive 30 <user>

Notes:

You can also check this setting in /etc/shadow directly. The 7th field should be 30 or less for all users with a password.

Note: A value of -1 would disable this setting.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV6	16.1
CSCV6	16.6
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3

QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/useradd -D | /bin/grep INACTIVE expect: ^INACTIVE=(30|[1-2][0-9]|[1-9])$ system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/useradd -D | /bin/grep INACTIVE' returned :

INACTIVE=-1
```

5.4.1.4 Ensure inactive password lock is 30 days or less - users

Info

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Solution

Run the following command to set the default password inactivity period to 30 days:

useradd -D -f 30

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

chage --inactive 30 <user>

Notes:

You can also check this setting in /etc/shadow directly. The 7th field should be 30 or less for all users with a password.

Note: A value of -1 would disable this setting.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV6	16.1
CSCV6	16.6
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3

QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^([^:]*:){6}(30|[1-2][0-9]|[1-9]):

file: /etc/shadow regex: ^[^:]+:[^!*] system: Linux

Hosts

192.168.56.115

```
Non-compliant file(s):
      /etc/shadow - regex '^[^:]+:[^!*]' found - expect '^([^:]*:){6}(30|[1-2][0-9]|[1-9]):' not
 found in the following lines:
          1: root:$y$j9T$ZAqGpmZL3dXmFzpLMRTKx0$x7nVBwwUPiI4A595o/
jLRCAUWT10oiGJdT3OnMFV04.:19570:0:99999:7:::
          36: vboxuser:$y$j9T$O5FXW0Or0OEDOaH5WFYR/0$XG7pxQmdZn.DNX/nilAfUUvOCJnLnD3t4fHRe1/
Z/53:19564:0:99999:7:::
```

5.4.4 Ensure default user umask is 027 or more restrictive - /etc/bash.bashrc

Info

The default umask determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile , .bashrc , etc.) in their home directories.

Rationale:

Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions. A default umask setting of 077 causes files and directories created by users to not be readable by any other user on the system. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

Solution

Edit the /etc/bash.bashrc, /etc/profile and /etc/profile.d/*.sh files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:

umask 027

Notes:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked.

Other methods of setting a default user umask exist however the shell configuration files are the last run and will override other settings if they exist therefor our recommendation is to configure in the shell configuration files. If other methods are in use in your environment they should be audited and the shell configs should be verified to not override.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4

CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*umask[\s]+[0-7][2-7]7[\s]*$ file: /etc/bash.bashrc regex: ^[\s]*umask[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/bash.bashrc" does not contain "^[\s]*umask[\s]"
```

5.4.4 Ensure default user umask is 027 or more restrictive - /etc/profile

Info

The default umask determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile , .bashrc , etc.) in their home directories.

Rationale:

Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions. A default umask setting of 077 causes files and directories created by users to not be readable by any other user on the system. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

Solution

Edit the /etc/bash.bashrc, /etc/profile and /etc/profile.d/*.sh files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:

umask 027

Notes:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked.

Other methods of setting a default user umask exist however the shell configuration files are the last run and will override other settings if they exist therefor our recommendation is to configure in the shell configuration files. If other methods are in use in your environment they should be audited and the shell configs should be verified to not override.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4

CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*umask[\s]+[0-7][2-7]7[\s]*$ file: /etc/profile regex: ^[\s]*umask[\s] system: Linux

Hosts

192.168.56.115

```
The file "/etc/profile" does not contain "^[\s]*umask[\s]"
```

5.4.5 Ensure default user shell timeout is 900 seconds or less

Info

The default TMOUT determines the shell timeout for users. The TMOUT value is measured in seconds.

Rationale:

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

Solution

Edit the /etc/bash.bashrc, /etc/profile and /etc/profile.d/*.sh files (and the appropriate files for any other shell supported on your system) and add or edit any TMOUT parameters in accordance with site policy:

readonly TMOUT=900 ; export TMOUT

Note: setting the value to readonly prevents unwanted modification during runtime.

Notes:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked. Other methods of setting a timeout exist for other shells not covered here.

Ensure that the timeout conforms to your local policy.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.10
800-53	AC-11
800-53R5	AC-11
CN-L3	8.1.4.1(b)
CSCV7	16.11
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-11
LEVEL	1S
NIAV2	AM23c
NIAV2	AM23d
PCI-DSSV3.2.1	8.1.8

PCI-DSSV4.0 8.2.8

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(readonly[\s]+)?TMOUT[\s]*=[\s]*([1-9]|[1-9][0-9]|[1-8][0-9]{2}|900)(;|[\s]|$) file: /etc/bash.bashrc /etc/profile /etc/profile.d/*.sh regex: ^[\s]*(readonly[\s]+)?TMOUT[\s]*=[\s]* system: Linux

Hosts

192.168.56.115

```
The file "/etc/bash.bashrc" does not contain "^[\s]*(readonly[\s]+)?TMOUT[\s]*=[\s]*"
```

Compliance 'SKIPPED'

Compliance 'PASSED'

1.1.1.1 Ensure mounting of freevxfs filesystems is disabled - lsmod

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/freevxfs.conf and add the following line:

install freevxfs /bin/true

Run the following command to unload the freevxfs module:

rmmod freevxfs

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/lsmod | /bin/grep freevxfs | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/lsmod | /bin/grep freevxfs | /usr/bin/awk '{print} END {if (NR == 0) print
 "pass" ; else print "fail"}'' returned :

pass
```

1.1.1.2 Ensure mounting of jffs2 filesystems is disabled - lsmod

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/jffs2.conf and add the following line:

install jffs2 /bin/true

Run the following command to unload the jffs2 module:

rmmod jffs2

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/lsmod | /bin/grep jffs2 | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.56.115

```
The command '/sbin/lsmod | /bin/grep jffs2 | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ;
 else print "fail"}'' returned :

pass
```

1.1.1.3 Ensure mounting of hfs filesystems is disabled - lsmod

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/hfs.conf and add the following line:

install hfs /bin/true

Run the following command to unload the hfs module:

rmmod hfs

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/lsmod | /bin/grep hfs | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.56.115

```
The command '/sbin/lsmod | /bin/grep hfs | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ;
 else print "fail"}'' returned :

pass
```

1.1.1.4 Ensure mounting of hfsplus filesystems is disabled - lsmod

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/hfsplus.conf and add the following line:

install hfsplus /bin/true

Run the following command to unload the hfsplus module:

rmmod hfsplus

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/lsmod | /bin/grep hfsplus | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.56.115

```
The command '/sbin/lsmod | /bin/grep hfsplus | /usr/bin/awk '{print} END {if (NR == 0) print
 "pass" ; else print "fail"}'' returned :

pass
```

1.1.1.5 Ensure mounting of squashfs filesystems is disabled - lsmod

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/squashfs.conf and add the following line:

install squashfs /bin/true

Run the following command to unload the squashfs module:

rmmod squashfs

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/lsmod | /bin/grep squashfs | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.56.115

```
The command '/sbin/lsmod | /bin/grep squashfs | /usr/bin/awk '{print} END {if (NR == 0) print
 "pass" ; else print "fail"}'' returned :

pass
```

1.1.1.6 Ensure mounting of udf filesystems is disabled - lsmod

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/udf.conf and add the following line:

install udf /bin/true

Run the following command to unload the udf module:

rmmod udf

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/lsmod | /bin/grep udf | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.56.115

```
The command '/sbin/lsmod | /bin/grep udf | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ;
 else print "fail"}'' returned :

pass
```

1.1.15 Ensure nodev option set on /dev/shm partition

Info

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

Rationale:

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

Solution

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

Run the following command to remount /dev/shm :

mount -o remount,nodev /dev/shm

References:

https://manpages.debian.org/buster/initscripts/tmpfs.5.en.html

Notes:

The setting in /etc/default/rcS, if present, will still be used, but the setting in /etc/default/tmpfs will take precedence if enabled. If desired, the defaults may also be overridden with an entry in in /etc/fstab

/run/shm was previously /dev/shm, and a compatibility symlink or bind mount will be created to allow the old path to continue to function. If an fstab entry for /dev/shm exists instead of /run/shm, then /dev/shm will continue to be used.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep /dev/shm expect: [\s]*[,]?nodev system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep /dev/shm' returned :

tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
```

1.1.16 Ensure nosuid option set on /dev/shm partition

Info

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

Rationale:

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

Solution

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

Run the following command to remount /dev/shm :

mount -o remount,nosuid /dev/shm

Notes:

The setting in /etc/default/rcS, if present, will still be used, but the setting in /etc/default/tmpfs will take precedence if enabled. If desired, the defaults may also be overridden with an entry in in /etc/fstab

/run/shm was previously /dev/shm, and a compatibility symlink or bind mount will be created to allow the old path to continue to function. If an fstab entry for /dev/shm exists instead of /run/shm, then /dev/shm will continue to be used.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/mount | /bin/grep /dev/shm expect: [\s]*[,]?nosuid system: Linux

Hosts

192.168.56.115

```
The command '/bin/mount | /bin/grep /dev/shm' returned :

tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
```

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

Info

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

Rationale:

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

Solution

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

df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d (-perm -0002 -a ! -perm -1000) 2>/dev/null | xargs -I '{}' chmod a+t '{}'

Notes:

Some distributions may not support the --local option to df.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/df --local -P | /usr/bin/awk {'if (NR!=1) print $6'} | /usr/bin/xargs -I '{}' /usr/bin/find '{}' -xdev -type d \(-perm -0002 -a ! -perm -1000 \) 2>/dev/null | /usr/bin/awk '{print} END {if (NR == 0) print "none"}'

expect: none system: Linux

Hosts

192.168.56.115

```
The command '/bin/df --local -P | /usr/bin/awk {'if (NR!=1) print $6'} | /usr/bin/xargs -I '{}' /
usr/bin/find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null | /usr/bin/awk
 '{print} END {if (NR == 0) print "none"}'' returned :

none
```

1.1.22 Disable Automounting

Info

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

Rationale:

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

Solution

Run one of the following commands:

Run the following command to disable autofs :

systemctl --now disable autofs

OR Run the following command to remove autofs

apt purge autofs

Impact:

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

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

This control should align with the tolerance of the use of portable drives and optical media in the organization. On a server requiring an admin to manually mount media can be part of defense-in-depth to reduce the risk of unapproved software or information being introduced or proprietary software or information being exfiltrated. If admins commonly use flash drives and Server access has sufficient physical controls, requiring manual mounting may not increase security.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.2
800-171	3.14.4
800-171	3.14.5
800-53	SI-3
800-53R5	SI-3
CN-L3	7.1.3.6(b)

CN-L3	8.1.4.5
CN-L3	8.1.9.6(a)
CN-L3	8.1.9.6(b)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.7(a)
CN-L3	8.1.10.7(b)
CSCV6	9.1
CSCV7	8.4
CSCV7	8.5
CSF	DE.CM-4
CSF	DE.DP-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.2.1
ITSG-33	SI-3
LEVEL	1S
NIAV2	GS8a
PCI-DSSV3.2.1	5.1
PCI-DSSV3.2.1	5.1.1
PCI-DSSV4.0	5.2.1
QCSC-V1	3.2
QCSC-V1	5.2.3
QCSC-V1	8.2.1
TBA-FIISB	49.2.1
TBA-FIISB	49.2.2
TBA-FIISB	49.3.1
TBA-FIISB	49.3.2
TBA-FIISB	50.2.1
TBA-FIISB	51.2.4
TBA-FIISB	51.2.7

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

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

```
disabled
```

1.1.23 Disable USB Storage - lsmod

Info

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

Rationale:

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

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/usb_storage.conf and add the following line:

install usb-storage /bin/true

Run the following command to unload the usb-storage module:

rmmod usb-storage

Notes:

An alternative solution to disabling the usb-storage module may be found in USBGuard.

Use of USBGuard and construction of USB device policies should be done in alignment with site policy.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.2
800-171	3.14.4
800-171	3.14.5
800-53	SI-3
800-53R5	SI-3
CN-L3	7.1.3.6(b)
CN-L3	8.1.4.5
CN-L3	8.1.9.6(a)
CN-L3	8.1.9.6(b)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.7(a)
CN-L3	8.1.10.7(b)
CSCV7	8.4

CSCV7	8.5
CSF	DE.CM-4
CSF	DE.DP-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.2.1
ITSG-33	SI-3
LEVEL	1S
NIAV2	GS8a
PCI-DSSV3.2.1	5.1
PCI-DSSV3.2.1	5.1.1
PCI-DSSV4.0	5.2.1
QCSC-V1	3.2
QCSC-V1	5.2.3
QCSC-V1	8.2.1
TBA-FIISB	49.2.1
TBA-FIISB	49.2.2
TBA-FIISB	49.3.1
TBA-FIISB	49.3.2
TBA-FIISB	50.2.1
TBA-FIISB	51.2.4
TBA-FIISB	51.2.7

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/lsmod | /bin/grep usb-storage | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'

expect: pass system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/lsmod | /bin/grep usb-storage | /usr/bin/awk '{print} END {if (NR == 0) print
 "pass" ; else print "fail"}'' returned :

pass
```

1.3.1 Ensure sudo is installed

Info

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

Rationale:

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

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

Solution

Install sudo using the following command.

apt install sudo

OR

apt install sudo-ldap

References:

SUDO(8)

http://www.sudo.ws/

Notes:

Use the sudo-ldap package if you need LDAP support for sudoers.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2(9)
800-53R5	AC-2(9)
CN-L3	8.1.4.2(c)
CSCV7	4.3
CSF	PR.AC-1
CSF	PR.AC-4

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM16
PCI-DSSV3.2.1	8.5
PCI-DSSV4.0	8.2.2
PCI-DSSV4.0	8.2.3
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s sudo sudo-ldap 2>&1 expect: install[\s]+ok[\s]+installed system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s sudo sudo-ldap 2>&1' returned :

dpkg-query: package 'sudo-ldap' is not installed and no information is available
Package: sudo
Status: install ok installed
Priority: optional
Section: admin
Installed-Size: 6054
Maintainer: Sudo Maintainers <sudo@packages.debian.org>
Architecture: amd64
Version: 1.9.13p3-1+deb12u1
Replaces: sudo-ldap
Depends: libaudit1 (>= 1:2.2.1), libc6 (>= 2.34), libpam0g (>= 0.99.7.1), libselinux1 (>= 3.1~),
 zlib1g (>= 1:1.2.0.2), libpam-modules
Pre-Depends: init-system-helpers (>= 1.54~)
Conflicts: sudo-ldap
Conffiles:
 /etc/init.d/sudo 4fd40c92739a3bb2242df7cc6af126df
 /etc/pam.d/sudo 7fa5090826481c517f23faa1e21c77a8
 /etc/pam.d/sudo-i 95199b1f3d5a60bcf98058d9f8b70e70
 /etc/sudo.conf 8c714b777580faea54a2eb6d5f17ad1d
 /etc/sudo_logsrvd.conf ad0ba586da300ae3ba46312ad744a6e2
 /etc/sudoers da8bee36494c904ba767f0dd58920878
 /etc/sudoers.d/README 44c75ff004a18eeefdde4c998914d6d3
Description: Provide limited super user privileges to specific users
 Sudo is a program designed to allow a sysadmin to give limited root
 privileges to users and log root activity.  The basic philosophy is to give
 as few privileges as possible but still allow people to get their work done.
```

```
 .
 This version is built with minimal shared library dependencies, use the
 sudo-ldap package instead if you need LDAP support for sudoers.
Homepage: https://www.sudo.ws/

Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

1.3.2 Ensure sudo commands use pty

Info

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

Rationale:

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

Solution

edit the file /etc/sudoers or a file in /etc/sudoers.d/ with visudo -f and add the following line:

Defaults use_pty

References:

SUDO(8)

Notes:

visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks or parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2(9)
800-53R5	AC-2(9)
CN-L3	8.1.4.2(c)
CSCV7	4.3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM16
PCI-DSSV3.2.1	8.5
PCI-DSSV4.0	8.2.2

PCI-DSSV4.0	8.2.3
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -s -E '^[[:space:]]*Defaults[[:space:]]+([^#]+,[[:space:]]*)?use_pty' /etc/sudoers /etc/sudoers.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep -s -E '^[[:space:]]*Defaults[[:space:]]+([^#]+,[[:space:]]*)?use_pty' /
etc/sudoers /etc/sudoers.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print
 "fail"}'' returned :

/etc/sudoers:Defaultsuse_pty
pass
```

1.5.1 Ensure permissions on bootloader config are configured

Info

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

Rationale:

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

Solution

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

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

Notes:

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

Replace /boot/grub/grub.cfg with the appropriate grub configuration file for your environment

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /boot/grub/grub.cfg group: root mask: 177 owner: root system: Linux

Hosts

192.168.56.115

```
The file /boot/grub/grub.cfg with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/boot/grub/grub.cfg
```

1.5.3 Ensure authentication required for single user mode

Info

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

Rationale:

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

Solution

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

passwd root

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^root:[*!]:

file: /etc/shadow regex: ^root:

system: Linux

Hosts

192.168.56.115

```
Compliant file(s):
      /etc/shadow - regex '^root:' found - expect '^root:[\*!]:' not found in the following lines:
          1: root:$y$j9T$ZAqGpmZL3dXmFzpLMRTKx0$x7nVBwwUPiI4A595o/
jLRCAUWT10oiGJdT3OnMFV04.:19570:0:99999:7:::
```

1.6.1 Ensure XD/NX support is enabled

Info

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

Rationale:

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

Solution

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

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

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

Notes:

Ensure your system supports the XD or NX bit and has PAE support before implementing this recommendation as this may prevent it from booting if these are not supported by your hardware.

See Also

https://workbench.cisecurity.org/files/2658

References

800-53	SC-39
800-53	SI-16
800-53R5	SC-39
800-53R5	SI-16
CSCV7	8.3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
LEVEL	1S
QCSC-V1	5.2.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/journalctl | /bin/grep 'NX (Execute' 2>&1 expect: NX[\s]+\(Execute[\s]+Disable\)[\s]+protection: [\s]+active

Hosts

192.168.56.115

```
The command '/bin/journalctl | /bin/grep 'NX (Execute' 2>&1' returned :

Jul 26 10:07:05 debian11 kernel: NX (Execute Disable) protection: active
Jul 26 16:29:39 debian11 kernel: NX (Execute Disable) protection: active
Jul 26 16:38:46 debian11 kernel: NX (Execute Disable) protection: active
Aug 01 09:24:30 debian11 kernel: NX (Execute Disable) protection: active
```

1.6.2 Ensure address space layout randomization (ASLR) is enabled - sysctl

Info

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

Rationale:

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

Solution

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

kernel.randomize_va_space = 2

Run the following command to set the active kernel parameter:

sysctl -w kernel.randomize_va_space=2

See Also

https://workbench.cisecurity.org/files/2658

References

800-53	SC-39
800-53	SI-16
800-53R5	SC-39
800-53R5	SI-16
CSCV6	3.1
CSCV7	8.3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
LEVEL	1S
QCSC-V1	5.2.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl kernel.randomize_va_space expect: ^[\s]*kernel\.randomize_va_space[\s]*=[\s]*2[\s]*$

Hosts

192.168.56.115

```
The command '/sbin/sysctl kernel.randomize_va_space' returned :

kernel.randomize_va_space = 2
```

1.6.3 Ensure prelink is disabled

Info

prelinkis a program that modifies ELF shared libraries and ELF dynamically linked binaries in such a way that the time needed for the dynamic linker to perform relocations at startup significantly decreases.

Rationale:

The prelinking feature can interfere with the operation of AIDE, because it changes binaries. Prelinking can also increase the vulnerability of the system if a malicious user is able to compromise a common library such as libc.

Solution

Run the following command to restore binaries to normal:

prelink -ua

Uninstall prelink using the appropriate package manager or manual installation:

apt purge prelink

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53R5	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b

NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s prelink 2>&1 expect: ^[\s]*dpkg-query: package \'prelink\' is not installed and no information is available[\s]* system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s prelink 2>&1' returned :

dpkg-query: package 'prelink' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

1.6.4 Ensure core dumps are restricted - processsizemax

Info

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

Rationale:

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

Solution

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

* hard core 0

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

fs.suid_dumpable = 0

Run the following command to set the active kernel parameter:

sysctl -w fs.suid_dumpable=0

If systemd-coredump is installed:

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

Storage=none ProcessSizeMax=0

Run the command:

systemctl daemon-reload

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6

LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

1.6.4 Ensure core dumps are restricted - storage

Info

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

Rationale:

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

Solution

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

* hard core 0

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

fs.suid_dumpable = 0

Run the following command to set the active kernel parameter:

sysctl -w fs.suid_dumpable=0

If systemd-coredump is installed:
edit /etc/systemd/coredump.conf and add/modify the following lines:

Storage=none ProcessSizeMax=0

Run the command:

systemctl daemon-reload

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6

LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

1.6.4 Ensure core dumps are restricted - sysctl

Info

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

Rationale:

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

Solution

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

* hard core 0

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

fs.suid_dumpable = 0

Run the following command to set the active kernel parameter:

sysctl -w fs.suid_dumpable=0

If systemd-coredump is installed:

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

Storage=none ProcessSizeMax=0

Run the command:

systemctl daemon-reload

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6

LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl fs.suid_dumpable expect: ^[\s]*fs\.suid_dumpable[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl fs.suid_dumpable' returned :

fs.suid_dumpable = 0
```

1.7.1.1 Ensure AppArmor is installed

Info

AppArmor provides Mandatory Access Controls.

Rationale:

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

Solution

Install Apparmor.

apt install apparmor

apt install apparmor-utils

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5

NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s apparmor | /bin/grep Status: 2>&1 expect: ^[\s]*Status: install ok installed[\s]* system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s apparmor | /bin/grep Status: 2>&1' returned :

Status: install ok installed
```

1.7.1.3 Ensure all AppArmor Profiles are in enforce or complain mode - 0 processes are unconfined

Info

AppArmor profiles define what resources applications are able to access.

Rationale:

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

Solution

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

aa-enforce /etc/apparmor.d/*

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

aa-complain /etc/apparmor.d/*

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3

LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/apparmor_status expect: ^[\s]*0[\s]+processes[\s]+are[\s]+unconfined system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/apparmor_status' returned :

apparmor module is loaded.
24 profiles are loaded.
22 profiles are in enforce mode.
   /usr/bin/evince
   /usr/bin/evince-previewer
   /usr/bin/evince-previewer//sanitized_helper
   /usr/bin/evince-thumbnailer
   /usr/bin/evince//sanitized_helper
   /usr/bin/man
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/NetworkManager/nm-dhcp-helper
   /usr/lib/connman/scripts/dhclient-script
   /usr/lib/cups/backend/cups-pdf
   /usr/sbin/cups-browsed
   /usr/sbin/cupsd
   /usr/sbin/cupsd//third_party
   /{,usr/}sbin/dhclient
   libreoffice-senddoc
   libreoffice-soffice//gpg
   libreoffice-xpdfimport
   lsb_release
   man_filter
   man_groff
   nvidia_modprobe
   nvidia_modprobe//kmod
2 profiles are in complain mode.
```

```
   libreoffice-oosplash
   libreoffice-soffice
0 profiles are in kill mode.
0 profiles are in unconfined mode.
2 processes have profiles defined.
2 processes are in enforce mode.
   /usr/sbin/cups-browsed (606)
   /usr/sbin/cupsd (554)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
0 processes are in mixed mode.
0 processes are in kill mode.
```

1.7.1.3 Ensure all AppArmor Profiles are in enforce or complain mode - profiles loaded

Info

AppArmor profiles define what resources applications are able to access.

Rationale:

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

Solution

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

aa-enforce /etc/apparmor.d/*

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

aa-complain /etc/apparmor.d/*

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3

LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/apparmor_status expect: ^[\s]*[1-9][0-9]*[\s]+profiles[\s]+are[\s]+loaded system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/apparmor_status' returned :

apparmor module is loaded.
24 profiles are loaded.
22 profiles are in enforce mode.
   /usr/bin/evince
   /usr/bin/evince-previewer
   /usr/bin/evince-previewer//sanitized_helper
   /usr/bin/evince-thumbnailer
   /usr/bin/evince//sanitized_helper
   /usr/bin/man
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/NetworkManager/nm-dhcp-helper
   /usr/lib/connman/scripts/dhclient-script
   /usr/lib/cups/backend/cups-pdf
   /usr/sbin/cups-browsed
   /usr/sbin/cupsd
   /usr/sbin/cupsd//third_party
   /{,usr/}sbin/dhclient
   libreoffice-senddoc
   libreoffice-soffice//gpg
   libreoffice-xpdfimport
   lsb_release
   man_filter
   man_groff
   nvidia_modprobe
   nvidia_modprobe//kmod
2 profiles are in complain mode.
```

```
   libreoffice-oosplash
   libreoffice-soffice
0 profiles are in kill mode.
0 profiles are in unconfined mode.
2 processes have profiles defined.
2 processes are in enforce mode.
   /usr/sbin/cups-browsed (606)
   /usr/sbin/cupsd (554)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
0 processes are in mixed mode.
0 processes are in kill mode.
```

1.8.1.4 Ensure permissions on /etc/motd are configured

Info

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

Rationale:

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

Solution

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

chown root:root /etc/motd

chmod u-x,go-wx /etc/motd

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/motd group: root mask: 133 owner: root required: NO system: Linux

Hosts

192.168.56.115

```
The file /etc/motd with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven permissions :
 FALSE is compliant with the policy value

/etc/motd
```

1.8.1.5 Ensure permissions on /etc/issue are configured

Info

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

Rationale:

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

Solution

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

chown root:root /etc/issue

chmod u-x,go-wx /etc/issue

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/issue group: root mask: 133 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/issue with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven permissions :
 FALSE is compliant with the policy value

/etc/issue
```

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

Info

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

Rationale:

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

Solution

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

chown root:root /etc/issue.net

chmod u-x,go-wx /etc/issue.net

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/issue.net group: root mask: 133 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/issue.net with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/issue.net
```

2.1.1 Ensure xinetd is not installed

Info

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

Rationale:

If there are no xinetd services required, it is recommended that the package be removed.

Solution

Run the following commands to remove xinetd:

apt purge xinetd

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3

CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s xinetd 2>&1 expect: ^[\s]*dpkg-query: package \'xinetd\' is not installed and no information is available[\s]* system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s xinetd 2>&1' returned :

dpkg-query: package 'xinetd' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

2.1.2 Ensure openbsd-inetd is not installed

Info

The inetd daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests.

Rationale:

If there are no inetd services required, it is recommended that the daemon be removed.

Solution

Run the following command to uninstall openbsd-inetd:

apt purge openbsd-inetd

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8

CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s openbsd-inetd 2>&1 expect: ^[\s]*dpkg-query: package \'openbsd-inetd\' is not installed and no information is available[\s]* system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s openbsd-inetd 2>&1' returned :

dpkg-query: package 'openbsd-inetd' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

2.2.1.1 Ensure time synchronization is in use

Info

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

Rationale:

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

Solution

On systems where host based time synchronization is not available, configure systemd-timesyncd. If 'full featured' and/or encrypted time synchronization is required, install chrony or NTP.

To install chrony:

atp install chrony

To install ntp:

apt install ntp

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

Notes:

systemd-timesyncd is part of systemd. Some versions of systemd have been compiled without systemd-timesycnd. On these distributions, chrony or NTP should be used instead of systemd-timesycnd.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.7
800-53	AU-8
800-53R5	AU-8
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1S

NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

2.2.1.2 Ensure systemd-timesyncd is configured - systemctl

Info

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network. It implements an SNTP client. In contrast to NTP implementations such as chrony or the NTP reference server this only implements a client side, and does not bother with the full NTP complexity, focusing only on querying time from one remote server and synchronizing the local clock to it. The daemon runs with minimal privileges, and has been hooked up with networkd to only operate when network connectivity is available. The daemon saves the current clock to disk every time a new NTP sync has been acquired, and uses this to possibly correct the system clock early at bootup, in order to accommodate for systems that lack an RTC such as the Raspberry Pi and embedded devices, and make sure that time monotonically progresses on these systems, even if it is not always correct. To make use of this daemon a new system user and group 'systemd-timesync' needs to be created on installation of systemd.

Note: The systemd-timesyncd service specifically implements only SNTP. This minimalistic service will set the system clock for large offsets or slowly adjust it for smaller deltas. More complex use cases are not covered by systemd-timesyncd.

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

Rationale:

Proper configuration is vital to ensuring time synchronization is working properly.

Solution

Run the following command to enable systemd-timesyncd

systemctl enable systemd-timesyncd.service

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

NTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org #Servers listed should be In Accordence With Local Policy

FallbackNTP=2.debian.pool.ntp.org 3.debian.pool.ntp.org #Servers listed should be In Accordence With Local Policy

RootDistanceMax=1 #should be In Accordence With Local Policy

Run the following commands to start systemd-timesyncd.service

systemctl start systemd-timesyncd.service

timedatectl set-ntp true

Notes:

some versions of systemd have been compiled without systemd-timesycnd. On these distributions, chrony or NTP should be used instead of systemd-timesycnd.

Not all options are avalible on all versions of systemd-timesyncd

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.7
800-53	AU-8
800-53R5	AU-8
CN-L3	8.1.4.3(b)
CSCV6	9.1
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1NS
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/systemctl is-enabled systemd-timesyncd.service expect: enabled system: Linux

Hosts

192.168.56.115

```
The command '/bin/systemctl is-enabled systemd-timesyncd.service' returned :

enabled
```

2.2.1.3 Ensure chrony is configured - ntp server

Info

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

Rationale:

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

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

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

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

server <remote-server>

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.7
800-53	AU-8
800-53R5	AU-8
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1S
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

2.2.1.3 Ensure chrony is configured - user

Info

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

Rationale:

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

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

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

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

server <remote-server>

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.7
800-53	AU-8
800-53R5	AU-8
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1S
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

2.2.1.4 Ensure ntp is configured - RUNASUSER

Info

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

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

Rationale:

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

Solution

Add or edit restrict lines in /etc/ntp.conf to match the following:

restrict -4 default kod nomodify notrap nopeer noquery restrict -6 default kod nomodify notrap nopeer noquery

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

server <remote-server>

Configure ntp to run as the ntp user by adding or editing the /etc/init.d/ntp file:

RUNASUSER=ntp

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.7
800-53	AU-8
800-53R5	AU-8
CN-L3	8.1.4.3(b)
CSCV6	3.1
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1S
NESA	T3.6.2

QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

2.2.1.4 Ensure ntp is configured - restrict -4

Info

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

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

Rationale:

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

Solution

Add or edit restrict lines in /etc/ntp.conf to match the following:

restrict -4 default kod nomodify notrap nopeer noquery restrict -6 default kod nomodify notrap nopeer noquery

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

server <remote-server>

Configure ntp to run as the ntp user by adding or editing the /etc/init.d/ntp file:

RUNASUSER=ntp

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.7
800-53	AU-8
800-53R5	AU-8
CN-L3	8.1.4.3(b)
CSCV6	3.1
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1S
NESA	T3.6.2

QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

2.2.1.4 Ensure ntp is configured - restrict -6

Info

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

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

Rationale:

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

Solution

Add or edit restrict lines in /etc/ntp.conf to match the following:

restrict -4 default kod nomodify notrap nopeer noquery restrict -6 default kod nomodify notrap nopeer noquery

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

server <remote-server>

Configure ntp to run as the ntp user by adding or editing the /etc/init.d/ntp file:

RUNASUSER=ntp

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.7
800-53	AU-8
800-53R5	AU-8
CN-L3	8.1.4.3(b)
CSCV6	3.1
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1S
NESA	T3.6.2

QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

2.2.2 Ensure X Window System is not installed

Info

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

Rationale:

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

Solution

Remove the X Windows System packages:

apt purge xserver-xorg*

Impact:

Many Linux systems run applications which require a Java runtime. Some Linux Java packages have a dependency on specific X Windows xorg-x11-fonts. One workaround to avoid this dependency is to use the 'headless' Java packages for your specific Java runtime, if provided by your distribution.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.9
800-53	CM-11
800-53R5	CM-11
CSCV7	2.6
CSF	DE.CM-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.2
LEVEL	1S
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -l xserver-xorg* expect: ^[\s]*(un[\s]+xserver-xorg.*<none>[\s]+<none>.*|dpkg-query: package \'xserver-xorg.*\' is not installed and no information is available|dpkg-query: no packages found matching xserver-xorg.*) system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -l xserver-xorg*' returned :

Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name                           Version                  Architecture Description
+++-==============================-========================-============-
=================================================
ii  xserver-xorg                   1:7.7+23                 amd64        X.Org X server
ii  xserver-xorg-core              2:21.1.7-3               amd64        Xorg X server - core server
un  xserver-xorg-driver-all       <none>                   <none>       (no description available)
ii  xserver-xorg-input-all         1:7.7+23                 amd64        X.Org X server -- input
 driver metapackage
un  xserver-xorg-input-evtouch    <none>                   <none>       (no description available)
ii  xserver-xorg-input-libinput    1.2.1-1+b1               amd64        X.Org X server -- libinput
 input driver
ii  xserver-xorg-input-wacom       1.1.0-1                  amd64        X.Org X server -- Wacom
 input driver
ii  xserver-xorg-legacy            2:21.1.7-3               amd64        setuid root Xorg server
 wrapper
ii  xserver-xorg-video-all         1:7.7+23                 amd64        X.Org X server -- output
 driver metapackage
ii  xserver-xorg-video-amdgpu      23.0.0-1                 amd64        X.Org X server -- AMDGPU
 display driver
ii  xserver-xorg-video-ati         1:19.1.0-3               amd64        X.Org X server -- AMD/ATI
 display driver wrapper
ii  xserver-xorg-video-fbdev       1:0.5.0-2                amd64        X.Org X server -- fbdev
 display driver
ii  xserver-xorg-video-intel       2:2.99.917+git20210115-1 amd64        X.Org X server -- Intel
 i8xx, i9xx display driver
un  xserver-xorg-video-mach64      <none>                   <none>       (no description available)
un  xserver-xorg-video-modesetting <none>                   <none>       (no descri [...]
```

2.2.5 Ensure DHCP Server is not enabled - dhcpd

Info

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses.

Rationale:

Unless a system is specifically set up to act as a DHCP server, it is recommended that this service be deleted to reduce the potential attack surface.

Solution

Run one of the following commands to disable dhcpd:

systemctl --now disable isc-dhcp-server

systemctl --now disable isc-dhcp-server6

References:

More detailed documentation on DHCP is available at http://www.isc.org/software/dhcp.

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1

CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

Failed to get unit file state for isc-dhcp-server.service: No such file or directory
disabled
```

2.2.5 Ensure DHCP Server is not enabled - isc-dhcp-server6

Info

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses.

Rationale:

Unless a system is specifically set up to act as a DHCP server, it is recommended that this service be deleted to reduce the potential attack surface.

Solution

Run one of the following commands to disable dhcpd:

systemctl --now disable isc-dhcp-server

systemctl --now disable isc-dhcp-server6

References:

More detailed documentation on DHCP is available at http://www.isc.org/software/dhcp.

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1

CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

Failed to get unit file state for isc-dhcp-server6.service: No such file or directory
disabled
```

2.2.6 Ensure LDAP server is not enabled

Info

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

Rationale:

If the system will not need to act as an LDAP server, it is recommended that the software be disabled to reduce the potential attack surface.

Solution

Run one of the following commands to disable slapd:

systemctl --now disable slapd

References:

For more detailed documentation on OpenLDAP, go to the project homepage at http://www.openldap.org.

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6

CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

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

2.2.7 Ensure NFS and RPC are not enabled - nfs-server

Info

The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network.

Rationale:

If the system does not export NFS shares or act as an NFS client, it is recommended that these services be disabled to reduce the remote attack surface.

Solution

Run the following commands to disable nfs and rpcbind:

systemctl --now disable nfs-server

systemctl --now disable rpcbind

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6

CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

Failed to get unit file state for nfs-server.service: No such file or directory
disabled
```

2.2.7 Ensure NFS and RPC are not enabled - rpcbind

Info

The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network.

Rationale:

If the system does not export NFS shares or act as an NFS client, it is recommended that these services be disabled to reduce the remote attack surface.

Solution

Run the following commands to disable nfs and rpcbind:

systemctl --now disable nfs-server

systemctl --now disable rpcbind

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6

CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

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

2.2.8 Ensure DNS Server is not enabled

Info

The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network.

Rationale:

Unless a system is specifically designated to act as a DNS server, it is recommended that the package be deleted to reduce the potential attack surface.

Solution

Run the following commands to disable DNS server:

systemctl --now disable bind9

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2

CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

Failed to get unit file state for bind9.service: No such file or directory
disabled
```

2.2.9 Ensure FTP Server is not enabled

Info

The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files.

Rationale:

FTP does not protect the confidentiality of data or authentication credentials. It is recommended SFTP be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be deleted to reduce the potential attack surface.

Solution

Run the following command to disable vsftpd:

systemctl --now disable vsftpd

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Additional FTP servers also exist and should be audited.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6

CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

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

2.2.10 Ensure HTTP server is not enabled

Info

HTTP or web servers provide the ability to host web site content.

Rationale:

Unless there is a need to run the system as a web server, it is recommended that the package be deleted to reduce the potential attack surface.

Solution

Run the following command to disable apache:

systemctl --now disable apache2

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Several httpd servers exist and can use other service names. apache, apache2, lighttpd, and nginx are example services that provide an HTTP server. These and other services should also be audited.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7

CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

Failed to get unit file state for apache2.service: No such file or directory
disabled
```

2.2.11 Ensure email services are not enabled

Info

dovecot is an open source mail submission and transport server for Linux based systems.

Rationale:

Unless mail transport services are to be provided by this system, it is recommended that the service be disabled or deleted to reduce the potential attack surface.

Solution

Run one of the following commands to disable dovecot :

systemctl --now disable dovecot

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Several IMAP/POP3 servers exist and can use other service names. courier-imap and cyrus-imap are example services that provide a mail server. These and other services should also be audited.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7

CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

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

2.2.12 Ensure Samba is not enabled

Info

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Server Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems.

Rationale:

If there is no need to mount directories and file systems to Windows systems, then this service can be deleted to reduce the potential attack surface.

Solution

Run the following command to disable Samba:

systemctl --now disable smbd

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7

CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

Failed to get unit file state for smbd.service: No such file or directory
disabled
```

2.2.13 Ensure HTTP Proxy Server is not enabled

Info

Squid is a standard proxy server used in many distributions and environments.

Rationale:

If there is no need for a proxy server, it is recommended that the squid proxy be deleted to reduce the potential attack surface.

Solution

Run the following command to disable squid:

systemctl --now disable squid

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

On some distributions the squid service is known as squid3, not squid. Several HTTP proxy servers exist. These and other services should be checked.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7

CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

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

2.2.14 Ensure SNMP Server is not enabled

Info

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

Rationale:

The SNMP server can communicate using SNMP v1, which transmits data in the clear and does not require authentication to execute commands. Unless absolutely necessary, it is recommended that the SNMP service not be used. If SNMP is required the server should be configured to disallow SNMP v1.

Solution

Run the following command to disable snmpd:

systemctl --now disable snmpd

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7

CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: disabled system: Linux

Hosts

192.168.56.115

```
The command returned :

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

2.2.15 Ensure mail transfer agent is configured for local-only mode - /etc/exim4/update-exim4.conf.conf

Info

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.

Rationale:

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

Solution

Edit /etc/exim4/update-exim4.conf.conf and and or modify following lines to look like the lines below:

dc_eximconfig_configtype='local'

dc_local_interfaces='127.0.0.1 ; ::1'

dc_readhost=''

dc_relay_domains=''

dc_minimaldns='false'

dc_relay_nets=''

dc_smarthost=''

dc_use_split_config='false'

dc_hide_mailname=''

dc_mailname_in_oh='true'

dc_localdelivery='mail_spool'

Restart exim4:

systemctl restart exim4

Notes:

This recommendation is designed around the exim4 mail server, depending on your environment you may have an alternative MTA installed such as sendmail. If this is the case consult the documentation for your installed MTA to configure the recommended state.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6

800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

2.2.15 Ensure mail transfer agent is configured for local-only mode - ss

Info

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.

Rationale:

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

Solution

Edit /etc/exim4/update-exim4.conf.conf and and or modify following lines to look like the lines below:

dc_eximconfig_configtype='local'

dc_local_interfaces='127.0.0.1 ; ::1'

dc_readhost=''

dc_relay_domains=''

dc_minimaldns='false'

dc_relay_nets=''

dc_smarthost=''

dc_use_split_config='false'

dc_hide_mailname=''

dc_mailname_in_oh='true'

dc_localdelivery='mail_spool'

Restart exim4:

systemctl restart exim4

Notes:

This recommendation is designed around the exim4 mail server, depending on your environment you may have an alternative MTA installed such as sendmail. If this is the case consult the documentation for your installed MTA to configure the recommended state.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7

800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

2.2.16 Ensure rsync service is not enabled

Info

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

Rationale:

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

Solution

Run the following command to disable rsync:

systemctl --now disable rsync

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4

CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s rsync | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'rsync' is not installed and no information is available system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s rsync | /bin/grep -E '(Status:|not installed)'' returned :

dpkg-query: package 'rsync' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

2.2.17 Ensure NIS Server is not enabled

Info

The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files.

Rationale:

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

Solution

Run the following command to disable nis:

systemctl --now disable nis

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6

CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s nis | /bin/grep -E '(Status:|not installed)'

expect: dpkg-query: package 'nis' is not installed and no information is available system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s nis | /bin/grep -E '(Status:|not installed)'' returned :

dpkg-query: package 'nis' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

2.3.1 Ensure NIS Client is not installed

Info

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client was used to bind a machine to an NIS server and receive the distributed configuration files.

Rationale:

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

Solution

Uninstall nis:

apt purge nis

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.9
800-53	CM-11
800-53R5	CM-11
CSCV7	2.6
CSF	DE.CM-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.2
LEVEL	1S
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s nis 2>&1 expect: ^[\s]*dpkg-query: package \'nis\' is not installed and no information is available[\s]* system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s nis 2>&1' returned :

dpkg-query: package 'nis' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

2.3.2 Ensure rsh client is not installed

Info

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

Rationale:

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

Solution

Uninstall rsh:

apt purge rsh-client

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.3
800-53	IA-2(1)
800-53R5	IA-2(1)
CN-L3	7.1.2.7(b)
CSCV7	4.5
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-2(1)
LEVEL	1S
NESA	T5.4.2
NIAV2	AM36
NIAV2	VL3c
QCSC-V1	5.2.2
QCSC-V1	13.2

SWIFT-CSCV1	1.2
TBA-FIISB	35.1
TBA-FIISB	36.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s rsh-client 2>&1 expect: ^[\s]*dpkg-query: package 'rsh-client' is not installed and no information is available[\s]* system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s rsh-client 2>&1' returned :

dpkg-query: package 'rsh-client' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

2.3.3 Ensure talk client is not installed

Info

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

Rationale:

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

Solution

Uninstall talk:

apt purge talk

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.9
800-53	CM-11
800-53R5	CM-11
CSCV7	2.6
CSF	DE.CM-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.2
LEVEL	1S
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s talk 2>&1 expect: ^[\s]*dpkg-query: package 'talk' is not installed and no information is available[\s]* system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s talk 2>&1' returned :

dpkg-query: package 'talk' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

2.3.4 Ensure telnet client is not installed

Info

The telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol.

Rationale:

The telnet protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The ssh package provides an encrypted session and stronger security and is included in most Linux distributions.

Solution

Uninstall telnet:

apt purge telnet

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.3
800-53	IA-2(1)
800-53R5	IA-2(1)
CN-L3	7.1.2.7(b)
CSCV7	4.5
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-2(1)
LEVEL	1S
NESA	T5.4.2
NIAV2	AM36
NIAV2	VL3c
QCSC-V1	5.2.2
QCSC-V1	13.2

SWIFT-CSCV1	1.2
TBA-FIISB	35.1
TBA-FIISB	36.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s telnet 2>&1 expect: ^[\s]*dpkg-query: package 'telnet' is not installed and no information is available[\s]* system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s telnet 2>&1' returned :

dpkg-query: package 'telnet' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

2.3.5 Ensure LDAP client is not installed

Info

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

Rationale:

If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.

Solution

Uninstall ldap-utils:

apt purge ldap-utils

Impact:

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

Notes:

The openldap-clients package can go by other names on some distributions. openldap2-client, and ldap-utils are known alternative package names.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.9
800-53	CM-11
800-53R5	CM-11
CSCV7	2.6
CSF	DE.CM-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.2
LEVEL	1S
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/dpkg -s ldap-utils 2>&1 expect: ^[\s]*dpkg-query: package 'ldap-utils' is not installed and no information is available[\s]* system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/dpkg -s ldap-utils 2>&1' returned :

dpkg-query: package 'ldap-utils' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

3.2.2 Ensure IP forwarding is disabled - ipv4 sysctl

Info

The net.ipv4.ip_forward and net.ipv6.conf.all.forwarding flags are used to tell the system whether it can forward packets or not.

Rationale:

Setting the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Solution

Run the following command to restore the default parameter and set the active kernel parameter:

grep -Els '^s*net.ipv4.ip_forwards*=s*1' /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while read filename; do sed -ri 's/^s*(net.ipv4.ip_forwards*)(=)(s*S+b).*$/# *REMOVED* 1/' $filename; done; sysctl -w net.ipv4.ip_forward=0; sysctl -w net.ipv4.route.flush=1

IF IPv6 is enabled:

Run the following command to restore the default parameter and set the active kernel parameter:

grep -Els '^s*net.ipv6.conf.all.forwardings*=s*1' /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while read filename; do sed -ri 's/^s*(net.ipv6.conf.all.forwardings*)(=)(s*S+b).*$/# *REMOVED* 1/' $filename; done; sysctl -w net.ipv6.conf.all.forwarding=0; sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.ip_forward expect: ^[\s]*net\.ipv4\.ip_forward[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.ip_forward' returned :

net.ipv4.ip_forward = 0
```

3.2.2 Ensure IP forwarding is disabled - ipv6 sysctl

Info

The net.ipv4.ip_forward and net.ipv6.conf.all.forwarding flags are used to tell the system whether it can forward packets or not.

Rationale:

Setting the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Solution

Run the following command to restore the default parameter and set the active kernel parameter:

grep -Els '^s*net.ipv4.ip_forwards*=s*1' /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while read filename; do sed -ri 's/^s*(net.ipv4.ip_forwards*)(=)(s*S+b).*$/# *REMOVED* 1/' $filename; done; sysctl -w net.ipv4.ip_forward=0; sysctl -w net.ipv4.route.flush=1

IF IPv6 is enabled:

Run the following command to restore the default parameter and set the active kernel parameter:

grep -Els '^s*net.ipv6.conf.all.forwardings*=s*1' /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while read filename; do sed -ri 's/^s*(net.ipv6.conf.all.forwardings*)(=)(s*S+b).*$/# *REMOVED* 1/' $filename; done; sysctl -w net.ipv6.conf.all.forwarding=0; sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv6.conf.all.forwarding expect: ^[\s]*net\.ipv6\.conf\.all\.forwarding[\s]*=[\s]*0[\s]*$
system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv6.conf.all.forwarding' returned :

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

3.3.1 Ensure source routed packets are not accepted - net.ipv4.conf.all.accept_source_route = 0

Info

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

Rationale:

Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6

CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.conf.all.accept_source_route expect: ^[\s]*net\.ipv4\.conf\.all \.accept_source_route[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.conf.all.accept_source_route' returned :

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

3.3.1 Ensure source routed packets are not accepted - net.ipv6.conf.all.accept_source_route = 0

Info

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

Rationale:

Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6

CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv6.conf.all.accept_source_route expect: ^[\s]*net\.ipv6\.conf\.all \.accept_source_route[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv6.conf.all.accept_source_route' returned :

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

3.3.1 Ensure source routed packets are not accepted - net.ipv6.conf.default.accept_source_route = 0

Info

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

Rationale:

Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Solution

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

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

Run the following commands to set the active kernel parameters:

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

IF IPv6 is enabled:

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

net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0

Run the following commands to set the active kernel parameters:

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6

CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv6.conf.default.accept_source_route expect: ^[\s]*net\.ipv6\.conf\.default \.accept_source_route[\s]*=[\s]*0[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv6.conf.default.accept_source_route' returned :

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

3.3.5 Ensure broadcast ICMP requests are ignored - net.ipv4.icmp_echo_ignore_broadcasts = 1

Info

Setting net.ipv4.icmp_echo_ignore_broadcasts to 1 will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses.

Rationale:

Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

Solution

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

net.ipv4.icmp_echo_ignore_broadcasts = 1

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1

sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.icmp_echo_ignore_broadcasts expect: ^[\s]*net \.ipv4\.icmp_echo_ignore_broadcasts[\s]*=[\s]*1[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.icmp_echo_ignore_broadcasts' returned :

net.ipv4.icmp_echo_ignore_broadcasts = 1
```

3.3.6 Ensure bogus ICMP responses are ignored - net.ipv4.icmp_ignore_bogus_error_responses = 1

Info

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

Rationale:

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

Solution

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

net.ipv4.icmp_ignore_bogus_error_responses = 1

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1

sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.icmp_ignore_bogus_error_responses expect: ^[\s]*net \.ipv4\.icmp_ignore_bogus_error_responses[\s]*=[\s]*1[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.icmp_ignore_bogus_error_responses' returned :

net.ipv4.icmp_ignore_bogus_error_responses = 1
```

3.3.8 Ensure TCP SYN Cookies is enabled - net.ipv4.tcp_syncookies = 1

Info

When tcp_syncookies is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

Rationale:

Attackers use SYN flood attacks to perform a denial of service attacked on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Solution

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

net.ipv4.tcp_syncookies = 1

Run the following commands to set the active kernel parameters:

sysctl -w net.ipv4.tcp_syncookies=1

sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/sysctl net.ipv4.tcp_syncookies expect: ^[\s]*net\.ipv4\.tcp_syncookies[\s]*=[\s]*1[\s]*$ system: Linux

Hosts

192.168.56.115

```
The command '/sbin/sysctl net.ipv4.tcp_syncookies' returned :

net.ipv4.tcp_syncookies = 1
```

3.5.1.1 Ensure a Firewall package is installed

Info

A Firewall package should be selected. Most firewall configuration utilities operate as a front end to nftables or iptables.

Rationale:

A Firewall package is required for firewall management and configuration.

Solution

Run one of the following commands to install the Firewall package that follows local site policy:

To install UFW, run the following command:

apt install ufw

To install nftables, run the following command:

apt install nftables

To install iptables, run the following command:

apt install iptables

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38

NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

3.5.2.1 Ensure ufw service is enabled - systemctl

Info

UncomplicatedFirewall (ufw) is a frontend for iptables. ufw provides a framework for managing netfilter, as well as a command-line and available graphical user interface for manipulating the firewall.

Ensure that the ufw service is enabled to protect your system.

Rationale:

The ufw service must be enabled and running in order for ufw to protect the system

Solution

Run the following command to enable ufw:

ufw enable

Impact:

Changing firewall settings while connected over network can result in being locked out of the system.

References:

http://manpages.ubuntu.com/manpages/precise/en/man8/ufw.8.html

Notes:

When running ufw enable or starting ufw via its initscript, ufw will flush its chains. This is required so ufw can maintain a consistent state, but it may drop existing connections (eg ssh). ufw does support adding rules before enabling the firewall.

Run the following command before running ufw enable.

ufw allow proto tcp from any to any port 22

The rules will still be flushed, but the ssh port will be open after enabling the firewall. Please note that once ufw is 'enabled', ufw will not flush the chains when adding or removing rules (but will when modifying a rule or changing the default policy).

By default, ufw will prompt when enabling the firewall while running under ssh. This can be disabled by using ufw --force enable.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)

CN-L3	8.1.10.6(j)
CSCV6	9.1
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

3.5.2.1 Ensure ufw service is enabled - ufw

Info

UncomplicatedFirewall (ufw) is a frontend for iptables. ufw provides a framework for managing netfilter, as well as a command-line and available graphical user interface for manipulating the firewall.

Ensure that the ufw service is enabled to protect your system.

Rationale:

The ufw service must be enabled and running in order for ufw to protect the system

Solution

Run the following command to enable ufw:

ufw enable

Impact:

Changing firewall settings while connected over network can result in being locked out of the system.

References:

http://manpages.ubuntu.com/manpages/precise/en/man8/ufw.8.html

Notes:

When running ufw enable or starting ufw via its initscript, ufw will flush its chains. This is required so ufw can maintain a consistent state, but it may drop existing connections (eg ssh). ufw does support adding rules before enabling the firewall.

Run the following command before running ufw enable.

ufw allow proto tcp from any to any port 22

The rules will still be flushed, but the ssh port will be open after enabling the firewall. Please note that once ufw is 'enabled', ufw will not flush the chains when adding or removing rules (but will when modifying a rule or changing the default policy).

By default, ufw will prompt when enabling the firewall while running under ssh. This can be disabled by using ufw --force enable.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)

CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

3.5.2.2 Ensure default deny firewall policy

Info

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

Rationale:

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

Solution

Run the following commands to implement a default deny policy:

ufw default deny incoming

ufw default deny outgoing

ufw default deny routed

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1

QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

3.5.2.3 Ensure loopback traffic is configured - allow in v4

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

ufw allow in on lo

ufw allow out from lo

sudo ufw deny in from 127.0.0.0/8

sudo ufw deny in from ::1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38

NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

3.5.2.3 Ensure loopback traffic is configured - allow in v6

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

ufw allow in on lo

ufw allow out from lo

sudo ufw deny in from 127.0.0.0/8

sudo ufw deny in from ::1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38

NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

3.5.2.3 Ensure loopback traffic is configured - allow out v4

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

ufw allow in on lo

ufw allow out from lo

sudo ufw deny in from 127.0.0.0/8

sudo ufw deny in from ::1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38

NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

3.5.2.3 Ensure loopback traffic is configured - allow out v6

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

ufw allow in on lo

ufw allow out from lo

sudo ufw deny in from 127.0.0.0/8

sudo ufw deny in from ::1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38

NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

3.5.2.3 Ensure loopback traffic is configured - deny in from 127.0.0.0/8

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

ufw allow in on lo

ufw allow out from lo

sudo ufw deny in from 127.0.0.0/8

sudo ufw deny in from ::1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38

NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

3.5.2.3 Ensure loopback traffic is configured - deny in from ::1

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:

ufw allow in on lo

ufw allow out from lo

sudo ufw deny in from 127.0.0.0/8

sudo ufw deny in from ::1

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38

NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

3.5.2.4 Ensure outbound connections are configured

Info

Configure the firewall rules for new outbound connections.

Rationale:

If rules are not in place for new outbound connections all packets will be dropped by the default policy preventing network usage.

Solution

Configure ufw in accordance with site policy. The following commands will implement a policy to allow all outbound connections on all interfaces:

ufw allow out on all

Notes:

Changing firewall settings while connected over network can result in being locked out of the system. Unlike iptables, when a new outbound rule is added, ufw automatically takes care of associated established connections, so no rules for the latter kind are required.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1NS
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26

PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

3.5.2.5 Ensure firewall rules exist for all open ports

Info

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Solution

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

ufw allow in <port>/<tcp or udp protocol>

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

The remediation command opens up the port to traffic from all sources. Consult ufw documentation and set any restrictions in compliance with site policy.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26

PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

3.5.3.5 Ensure outbound and established connections are configured

Info

Configure the firewall rules for new outbound, and established connections

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure nftables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

nft add rule inet filter input ip protocol tcp ct state established accept

nft add rule inet filter input ip protocol udp ct state established accept

nft add rule inet filter input ip protocol icmp ct state established accept

nft add rule inet filter output ip protocol tcp ct state new,related,established accept

nft add rule inet filter output ip protocol udp ct state new,related,established accept

nft add rule inet filter output ip protocol icmp ct state new,related,established accept

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)

LEVEL	1NS
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/nft list ruleset expect: system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/nft list ruleset' did not return any result
```

4.2.1.2 Ensure rsyslog Service is enabled

Info

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

Rationale:

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

Solution

Run the following commands to enable rsyslog:

systemctl --now enable rsyslog

Notes:

Additional methods of enabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV6	9.1
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)

ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - '*.*;mail.none;news.none -/var/log/messages'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3

800-53R5	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - '*.=warning;*.=err -/var/log/warn'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - '*.crit /var/log/warn'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - '*.emerg :omusrmsg:*'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - 'local0,local1.* -/var/log/localmessages'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - 'local2,local3.* -/var/log/localmessages'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - 'local4,local5.* -/var/log/localmessages'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - 'local6,local7.* -/var/log/localmessages'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - 'mail.* -/var/log/mail'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - 'mail.err /var/log/mail.err'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - 'mail.info -/var/log/mail.info'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - 'mail.warning -/var/log/mail.warn'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - 'news.crit -/var/log/news/news.crit'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - 'news.err -/var/log/news/news.err'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.3 Ensure logging is configured - 'news.notice -/var/log/news/news.notice'

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment:

.emerg :omusrmsg: auth,authpriv.* /var/log/auth.log mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice

.=warning;.=err -/var/log/warn

*.crit /var/log/warn

.;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

On some systems /var/log/secure should be used for authentication data rather than /var/log/auth.log. Please consult your distribution-specific recommendations for further details.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-12

CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.4 Ensure rsyslog default file permissions configured

Info

rsyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Rationale:

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

Solution

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and set $FileCreateMode to 0640 or more restrictive:

$FileCreateMode 0640

References:

See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

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

Info

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

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

Solution

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and add one of the following lines:

Newer syntax:

<files to sent to the remote log server> action(type='omfwd' target='<FQDN or ip of loghost>' port='<port number>' protocol='tcp'

action.resumeRetryCount='<number of re-tries>'

queue.type='linkList' queue.size=<number of messages to queue>')

Example:

. action(type='omfwd' target='192.168.2.100' port'514' protocol='tcp'

action.resumeRetryCount='100'

queue.type='linkList' queue.size='1000')

Older syntax:

. @@<FQDN or ip of loghost>

Example:

. @@192.168.2.100

Run the following command to reload the rsyslog configuration:

systemctl reload rsyslog

References:

See the rsyslog.conf(5) man page for more information.

Notes:

The double 'at' sign (@@) directs rsyslogto use TCP to send log messages to the server, which is a more reliable transport mechanism than the default UDP protocol.

. sends all logs to the remote loghost. Ensure that the selection of logfiles being sent follows local site policy

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-6
800-53R5	AU-6
CN-L3	7.1.3.3(d)
CSCV7	6.6
CSCV7	6.8
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.DP-4
CSF	PR.PT-1
CSF	RS.AN-1
CSF	RS.CO-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-6
LEVEL	1S
NESA	M5.2.5
QCSC-V1	5.2.3
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts - InputTCPServerRun 514

Info

By default, rsyslog does not listen for log messages coming in from remote systems. The ModLoad tells rsyslog to load the imtcp.so module so it can listen over a network via TCP. The InputTCPServerRun option instructs rsyslogd to listen on the specified TCP port.

Rationale:

The guidance in the section ensures that remote log hosts are configured to only accept rsyslog data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote rsyslog messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

Solution

For hosts that are designated as log hosts, edit the /etc/rsyslog.conf file and un-comment or add the following lines:

$ModLoad imtcp

$InputTCPServerRun 514

For hosts that are not designated as log hosts, edit the /etc/rsyslog.conf file and comment or remove the following lines:

$ModLoad imtcp

$InputTCPServerRun 514

Run the following command to reload the rsyslogd configuration:

systemctl restart rsyslog

References:

See the rsyslog(8) man page for more information.

Notes:

The $ModLoad imtcp line can have the .so extension added to the end of the module, or use the full path to the module.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7

800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts - ModLoad imtcp

Info

By default, rsyslog does not listen for log messages coming in from remote systems. The ModLoad tells rsyslog to load the imtcp.so module so it can listen over a network via TCP. The InputTCPServerRun option instructs rsyslogd to listen on the specified TCP port.

Rationale:

The guidance in the section ensures that remote log hosts are configured to only accept rsyslog data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote rsyslog messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

Solution

For hosts that are designated as log hosts, edit the /etc/rsyslog.conf file and un-comment or add the following lines:

$ModLoad imtcp

$InputTCPServerRun 514

For hosts that are not designated as log hosts, edit the /etc/rsyslog.conf file and comment or remove the following lines:

$ModLoad imtcp

$InputTCPServerRun 514

Run the following command to reload the rsyslogd configuration:

systemctl restart rsyslog

References:

See the rsyslog(8) man page for more information.

Notes:

The $ModLoad imtcp line can have the .so extension added to the end of the module, or use the full path to the module.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7

800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

5.1.1 Ensure cron daemon is enabled

Info

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

Rationale:

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

Solution

Based on your system configuration, run the appropriate one of the following commands to enable cron:

systemctl --now enable cron

Notes:

Additional methods of enabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-6
800-53R5	AU-6
CN-L3	7.1.3.3(d)
CSCV6	9.1
CSCV7	6
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.DP-4
CSF	PR.PT-1
CSF	RS.AN-1
CSF	RS.CO-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-6
LEVEL	1S
NESA	M5.2.5

QCSC-V1	5.2.3
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: enabled system: Linux

Hosts

192.168.56.115

```
The command returned :

enabled
```

5.1.8 Ensure at/cron is restricted to authorized users - at.deny

Info

Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. If /etc/cron.allow or /etc/at.allow do not exist, then /etc/at.deny and /etc/cron.deny are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in /etc/cron.allow and /etc/at.allow are allowed to use at and cron. Note that even though a given user is not listed in cron.allow , cron jobs can still be run as that user. The cron.allow file only controls administrative access to the crontab command for scheduling and modifying cron jobs.

Rationale:

On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Solution

Run the following commands to remove /etc/cron.deny, create /etc/cron.allow, and set permissions and ownership for /etc/cron.allow:

rm /etc/cron.deny # touch /etc/cron.allow # chown root:root /etc/cron.allow # chmod g-wx,o-rwx /etc/cron.allow

If at is installed on the system:

Run the following commands to remove /etc/at.deny; create /etc/at.allow, and set ownership and permissions on/etc/at.allow`:

rm /etc/at.deny # touch /etc/at.allow # chown root:root /etc/at.allow # chmod g-wx,o-rwx /etc/at.allow

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	9.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/at.deny system: Linux

Hosts

192.168.56.115

```
No files found: /etc/at.deny
```

5.1.8 Ensure at/cron is restricted to authorized users - cron.deny

Info

Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. If /etc/cron.allow or /etc/at.allow do not exist, then /etc/at.deny and /etc/cron.deny are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in /etc/cron.allow and /etc/at.allow are allowed to use at and cron. Note that even though a given user is not listed in cron.allow , cron jobs can still be run as that user. The cron.allow file only controls administrative access to the crontab command for scheduling and modifying cron jobs.

Rationale:

On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Solution

Run the following commands to remove /etc/cron.deny, create /etc/cron.allow, and set permissions and ownership for /etc/cron.allow:

rm /etc/cron.deny # touch /etc/cron.allow # chown root:root /etc/cron.allow # chmod g-wx,o-rwx /etc/cron.allow

If at is installed on the system:

Run the following commands to remove /etc/at.deny; create /etc/at.allow, and set ownership and permissions on/etc/at.allow`:

rm /etc/at.deny # touch /etc/at.allow # chown root:root /etc/at.allow # chmod g-wx,o-rwx /etc/at.allow

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	9.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/cron.deny system: Linux

Hosts

192.168.56.115

```
No files found: /etc/cron.deny
```

5.2.2 Ensure permissions on SSH private host key files are configured

Info

An SSH private key is one of two files used in SSH public key authentication. In this authentication method, The possession of the private key is proof of identity. Only a private key that corresponds to a public key will be able to authenticate successfully. The private keys need to be stored and handled carefully, and no copies of the private key should be distributed.

Rationale:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated

Solution

Run the following commands to set ownership and permissions on the private SSH host key files

find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chown root:root {} ;

find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chmod 0600 {} ;

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/ssh/*key mask: 177 system: Linux

Hosts

192.168.56.115

```
The file /etc/ssh/ssh_host_ecdsa_key with fmode owner: root group: root mode: 0600 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value
The file /etc/ssh/ssh_host_ed25519_key with fmode owner: root group: root mode: 0600 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value
The file /etc/ssh/ssh_host_rsa_key with fmode owner: root group: root mode: 0600 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value

/etc/ssh/ssh_host_ecdsa_key, /etc/ssh/ssh_host_ed25519_key, /etc/ssh/ssh_host_rsa_key
```

5.2.3 Ensure permissions on SSH public host key files are configured

Info

An SSH public key is one of two files used in SSH public key authentication. In this authentication method, a public key is a key that can be used for verifying digital signatures generated using a corresponding private key. Only a public key that corresponds to a private key will be able to authenticate successfully.

Rationale:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Solution

Run the following commands to set permissions and ownership on the SSH host public key files

find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chmod go-wx {} ;

find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chown root:root {} ;

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4

NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/ssh/*key.pub mask: 133 system: Linux

Hosts

192.168.56.115

```
The file /etc/ssh/ssh_host_ecdsa_key.pub with fmode owner: root group: root mode: 0644 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value
The file /etc/ssh/ssh_host_ed25519_key.pub with fmode owner: root group: root mode: 0644 uid: 0 gid:
 0 uneven permissions : FALSE is compliant with the policy value
The file /etc/ssh/ssh_host_rsa_key.pub with fmode owner: root group: root mode: 0644 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value

/etc/ssh/ssh_host_ecdsa_key.pub, /etc/ssh/ssh_host_ed25519_key.pub, /etc/ssh/ssh_host_rsa_key.pub
```

5.2.8 Ensure SSH IgnoreRhosts is enabled

Info

The IgnoreRhosts parameter specifies that .rhosts and .shosts files will not be used in RhostsRSAAuthentication or HostbasedAuthentication.

Rationale:

Setting this parameter forces users to enter a password when authenticating with ssh.

Solution

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

IgnoreRhosts yes

Default Value:

IgnoreRhosts yes

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
800-53R5	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5

CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^(?i)[\s]*ignorerhosts[\s]+no[\s]*$(?-i) file: /etc/ssh/sshd_config regex: ^(?i)[\s]*ignorerhosts[\s](?-i) system: Linux

Hosts

192.168.56.115

```
The file "/etc/ssh/sshd_config" does not contain "^(?i)[\s]*ignorerhosts[\s](?-i)"
```

5.2.13 Ensure only strong Ciphers are used

Info

This variable limits the ciphers that SSH can use during communication.

Rationale:

Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised

The DES, Triple DES, and Blowfish ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, aka a 'Sweet32' attack

The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the 'Bar Mitzvah' issue

The passwords used during an SSH session encrypted with RC4 can be recovered by an attacker who is able to capture and replay the session

Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors

The mm_newkeys_from_blob function in monitor_wrap.c, when an AES-GCM cipher is used, does not properly initialize memory for a MAC context data structure, which allows remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Edit the /etc/ssh/sshd_config file add/modify the Ciphers line to contain a comma separated list of the site approved ciphers Example:

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

Default Value:

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

References:

https://nvd.nist.gov/vuln/detail/CVE-2016-2183

https://nvd.nist.gov/vuln/detail/CVE-2015-2808

https://www.kb.cert.org/vuls/id/565052

https://www.openssh.com/txt/cbc.adv

https://nvd.nist.gov/vuln/detail/CVE-2008-5161

https://nvd.nist.gov/vuln/detail/CVE-2013-4548

https://www.kb.cert.org/vuls/id/565052

https://www.openssh.com/txt/cbc.adv

SSHD_CONFIG(5)

Notes:

Some organizations may have stricter requirements for approved ciphers. Ensure that ciphers used are in compliance with site policy.

The only 'strong' ciphers currently FIPS 140-2 compliant are: aes256-ctr,aes192-ctr,aes128-ctr

CVE-2013-4548 referenced above applies to OpenSSH versions 6.2 and 6.3. If running these versions of Open SSH, Please upgrade to version 6.4 or later to fix the vulnerability, or disable AES-GCM in the server configuration.

The Following are the supported ciphers in openSSH:

3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

aes128-ctr

aes192-ctr

aes256-ctr

aes128-gcm@openssh.com

aes256-gcm@openssh.com

arcfour

arcfour128

arcfour256

blowfish-cbc

cast128-cbc

rijndael-cbc@lysator.liu.se

chacha20-poly1305@openssh.com

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.8
800-53	SC-8
800-53R5	SC-8
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSCV7	14.4
CSF	PR.DS-2
CSF	PR.DS-5
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ITSG-33	SC-8
ITSG-33	SC-8a.
LEVEL	1S
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/sshd -T | /bin/grep ciphers | /bin/grep -oP '((3des-cbc|aes128-cbc|aes192-cbc|aes256-cbc|arcfour|arcfour128|arcfour256|blowfish-cbc|cast128-cbcz|rijndael-cbc@lysator.liu.se)[,]?)+' | /bin/awk '{print} END {if (NR == 0) print "pass"; else print $0 }'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/sshd -T | /bin/grep ciphers | /bin/grep -oP '((3des-cbc|aes128-cbc|aes192-
cbc|aes256-cbc|arcfour|arcfour128|arcfour256|blowfish-cbc|cast128-cbcz|rijndael-cbc@lysator.liu.se)
[,]?)+' | /bin/awk '{print} END {if (NR == 0) print "pass"; else print $0 }'' returned :

pass
```

5.2.15 Ensure only strong Key Exchange algorithms are used

Info

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received

Rationale:

Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Edit the /etc/ssh/sshd_config file add/modify the KexAlgorithms line to contain a comma separated list of the site approved key exchange algorithms Example:

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

Default Value:

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

Notes:

Kex algorithms have a higher preference the earlier they appear in the list

Some organizations may have stricter requirements for approved Key exchange algorithms. Ensure that Key exchange algorithms used are in compliance with site policy.

The only Key Exchange Algorithms currently FIPS 140-2 approved are: ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256

The Key Exchange algorithms supported by OpenSSH 7 are:

curve25519-sha256

curve25519-sha256@libssh.org

diffie-hellman-group1-sha1

diffie-hellman-group14-sha1

diffie-hellman-group-exchange-sha1

diffie-hellman-group-exchange-sha256

ecdh-sha2-nistp256

ecdh-sha2-nistp384

ecdh-sha2-nistp521

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.8
800-53	SC-8
800-53R5	SC-8
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSCV7	14.4
CSF	PR.DS-2
CSF	PR.DS-5
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ITSG-33	SC-8
ITSG-33	SC-8a.
LEVEL	1S
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24

PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/sshd -T | /bin/grep -i 'kexalgorithms' | /bin/grep -oP '((diffie-hellman-group1-sha1|diffie-hellman-group14-sha1|diffie-hellman-group-exchange-sha1)[,]?)+' | /bin/awk '{print} END {if (NR == 0) print "pass"; else print $0 }'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/sshd -T | /bin/grep -i 'kexalgorithms' | /bin/grep -oP '((diffie-hellman-
group1-sha1|diffie-hellman-group14-sha1|diffie-hellman-group-exchange-sha1)[,]?)+' | /bin/awk
 '{print} END {if (NR == 0) print "pass"; else print $0 }'' returned :

pass
```

5.2.16 Ensure SSH Idle Timeout Interval is configured - ClientAliveCountMax

Info

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

Rationale:

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

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

Solution

Edit the /etc/ssh/sshd_config file to set the parameters according to site policy:

ClientAliveInterval 300

ClientAliveCountMax 0

Default Value:

ClientAliveInterval 300

ClientAliveCountMax 0

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.10
800-53	AC-11
800-53R5	AC-11
CN-L3	8.1.4.1(b)
CSCV7	16.11
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO/IEC-27001	A.11.2.8

ITSG-33	AC-11
LEVEL	1S
NIAV2	AM23c
NIAV2	AM23d
PCI-DSSV3.2.1	8.1.8
PCI-DSSV4.0	8.2.8

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/sshd -T | /bin/grep clientalivecountmax expect: ^[\s]*clientalivecountmax[\s]+[0-3][\s]*$
system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/sshd -T | /bin/grep clientalivecountmax' returned :

clientalivecountmax 3
```

5.2.20 Ensure SSH PAM is enabled

Info

UsePAM Enables the Pluggable Authentication Module interface. If set to 'yes' this will enable PAM authentication using ChallengeResponseAuthentication and PasswordAuthentication in addition to PAM account and session module processing for all authentication types

Rationale:

When usePAM is set to yes, PAM runs through account and session types properly. This is important if you want to restrict access to services based off of IP, time or other factors of the account. Additionally, you can make sure users inherit certain environment variables on login or disallow access to the server

Solution

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

UsePAM yes

Impact:

If UsePAM is enabled, you will not be able to run sshd(8) as a non-root user.

Default Value:

usePAM yes

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(?i)usePAM(?-i)[\s]+yes[\s]*$ file: /etc/ssh/sshd_config regex: ^[\s]*(?i)usePAM(?-i)[\s] system: Linux

Hosts

192.168.56.115

```
Compliant file(s):
      /etc/ssh/sshd_config - regex '^[\s]*(?i)usePAM(?-i)[\s]' found - expect '^[\s]*(?i)usePAM(?-i)
[\s]+yes[\s]*$' found in the following lines:
          85: UsePAM yes
```

5.2.23 Ensure SSH MaxSessions is limited

Info

The MaxSessions parameter specifies the maximum number of open sessions permitted from a given connection.

Rationale:

To protect a system from denial of service due to a large number of concurrent sessions, use the rate limiting function of MaxSessions to protect availability of sshd logins and prevent overwhelming the daemon.

Solution

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

MaxSessions 10

Default Value:

MaxSessions 10

Notes:

Local site policy may be more restrictive

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*(?i)MaxSessions(?-i)[\s]+(10|[1-9])[\s]*$ file: /etc/ssh/sshd_config regex: ^[\s]*(?i)MaxSessions(?-i)[\s] string_required: NO system: Linux

Hosts

192.168.56.115

```
No matching files were found
```

5.3.2 Ensure lockout for failed password attempts is configured - pam_deny.so

Info

Lock out users after n unsuccessful consecutive login attempts. The first sets of changes are made to the PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM.

deny=n - n represents the number of failed attempts before the account is locked

unlock_time=n - n represents the number of seconds before the account is unlocked

audit - Will log the user name into the system log if the user is not found.

silent - Don't print informative messages.

Set the lockout number and unlock time in accordance with local site policy.

Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Solution

Edit the /etc/pam.d/common-auth file and add the auth line below:

auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900

Edit the /etc/pam.d/common-account file and add the account lines bellow:

account requisite pam_deny.so account required pam_tally2.so

Note: If a user has been locked out because they have reached the maximum consecutive failure count defined by deny= in the pam_tally2.so module, the user can be unlocked by issuing the command /sbin/pam_tally2 -u <username> --reset. This command sets the failed count to 0, effectively unlocking the user.

Notes:

BUG In pam_tally2.so

To work around this issue you have to add pam_tally2 to the account section account required pam_tally2.so for the counter to reset to 0 when using sudo

Use of the 'audit' keyword may log credentials in the case of user error during authentication. This risk should be evaluated in the context of the site policies of your organization.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2
800-53R5	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16.7
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*account[\s]+requisite[\s]+pam_deny\.so[\s]*$ file: /etc/pam.d/common-account regex: ^[\s]*account[\s]+requisite[\s]+pam_deny\.so[\s]* system: Linux

Hosts

192.168.56.115

```
Compliant file(s):
      /etc/pam.d/common-account - regex '^[\s]*account[\s]+requisite[\s]+pam_deny\.so[\s]*' found -
 expect '^[\s]*account[\s]+requisite[\s]+pam_deny\.so[\s]*$' found in the following lines:
          19: accountrequisitepam_deny.so
```

5.4.1.3 Ensure password expiration warning days is 7 or more - login.defs

Info

The PASS_WARN_AGE parameter in /etc/login.defs allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the PASS_WARN_AGE parameter be set to 7 or more days.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

Solution

Set the PASS_WARN_AGE parameter to 7 in /etc/login.defs :

PASS_WARN_AGE 7

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

chage --warndays 7 <user>

Notes:

You can also check this setting in /etc/shadow directly. The 6th field should be 7 or more for all users with a password.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2

SWIFT-CSCV1 4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*PASS_WARN_AGE[\s]+([7-9]|[1-9][0-9]+)[\s]*$ file: /etc/login.defs regex: ^[\s]*PASS_WARN_AGE[\s]+ system: Linux

Hosts

192.168.56.115

```
Compliant file(s):
      /etc/login.defs - regex '^[\s]*PASS_WARN_AGE[\s]+' found - expect
 '^[\s]*PASS_WARN_AGE[\s]+([7-9]|[1-9][0-9]+)[\s]*$' found in the following lines:
          167: PASS_WARN_AGE7
```

5.4.1.3 Ensure password expiration warning days is 7 or more - users

Info

The PASS_WARN_AGE parameter in /etc/login.defs allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the PASS_WARN_AGE parameter be set to 7 or more days.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

Solution

Set the PASS_WARN_AGE parameter to 7 in /etc/login.defs :

PASS_WARN_AGE 7

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

chage --warndays 7 <user>

Notes:

You can also check this setting in /etc/shadow directly. The 6th field should be 7 or more for all users with a password.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2

SWIFT-CSCV1 4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^([^:]*:){5}([7-9]|[1-9][0-9]+):

file: /etc/shadow regex: ^[^:]+:[^!*] system: Linux

Hosts

192.168.56.115

```
Compliant file(s):
      /etc/shadow - regex '^[^:]+:[^!*]' found - expect '^([^:]*:){5}([7-9]|[1-9][0-9]+):' found in
 the following lines:
          1: root:$y$j9T$ZAqGpmZL3dXmFzpLMRTKx0$x7nVBwwUPiI4A595o/
jLRCAUWT10oiGJdT3OnMFV04.:19570:0:99999:7:::
          36: vboxuser:$y$j9T$O5FXW0Or0OEDOaH5WFYR/0$XG7pxQmdZn.DNX/nilAfUUvOCJnLnD3t4fHRe1/
Z/53:19564:0:99999:7:::
```

5.4.1.5 Ensure all users last password change date is in the past

Info

All users should have a password change date in the past.

Rationale:

If a users recorded password change date is in the future then they could bypass any set password expiration.

Solution

Investigate any users with a password change date in the future and correct them. Locking the account, expiring the password, or resetting the password manually may be appropriate.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: for user in $(cat /etc/shadow | cut -d: -f1); do expiry=$(date -d "$(chage --list $user | grep -Poi 'Last password changes*:[\s]*K((Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec)[\s]+[0-9]{1,2}, 2[0-9]

{3})$')" +%s); today=$(date +%s); if [$expiry -gt $today]; then echo "$user expiry date is in future"; fi ; done | /usr/bin/awk '{print} END {if (NR == 0) print "pass"; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command 'for user in $(cat /etc/shadow | cut -d: -f1); do expiry=$(date -d "$(chage --list
 $user | grep -Poi 'Last password changes*:[\s]*K((Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec)
[\s]+[0-9]{1,2}, 2[0-9]{3})$')" +%s); today=$(date +%s); if [ $expiry -gt $today ]; then echo "$user
 expiry date is in future"; fi ; done | /usr/bin/awk '{print} END {if (NR == 0) print "pass"; else
 print "fail"}'' returned :

pass
```

5.4.2 Ensure system accounts are secured

Info

There are a number of accounts provided with most distributions that are used to manage applications and are not intended to provide an interactive shell.

Rationale:

It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, most distributions set the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to the nologin shell. This prevents the account from potentially being used to run any commands.

Solution

Run the commands appropriate for your distribution:

Set the shell for any accounts returned by the audit to nologin:

usermod -s $(which nologin) <user>

Lock any non root accounts returned by the audit:

usermod -L <user>

The following command will set all system accounts to a non login shell:

awk -F: '($1!='root' && $1!='sync' && $1!='shutdown' && $1!='halt' && $1!~/^+/ && $3<''$(awk '/^s*UID_MIN/ {print $2}' /etc/login.defs)'' && $7!='"$(which nologin)"' && $7!='/bin/false') {print $1}' /etc/passwd | while read -r user; do usermod -s '$(which nologin)' '$user'; done

The following command will automatically lock not root system accounts:

awk -F: '($1!='root' && $1!~/^+/ && $3<''$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)'') {print $1}' /etc/ passwd | xargs -I '{}' passwd -S '{}' | awk '($2!='L' && $2!='LK') {print $1}' | while read -r user; do usermod -L '$user'; done

Notes:

The root, sync, shutdown, and halt users are exempted from requiring a non-login shell.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2
800-53R5	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16

CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/awk -F: '($1!="root" && $1!~/^\+/ && $3<'"$(/usr/bin/awk '/^[\s]*UID_MIN/{print $2}' /etc/login.defs)"') {print $1}' /etc/passwd | /usr/bin/xargs -I '{}' /usr/bin/passwd -S '{}' | /usr/bin/awk '($2!="L" && $2!="LK") {print $1}' | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'

expect: ^pass$ system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/awk -F: '($1!="root" && $1!~/^\+/ && $3<'"$(/usr/bin/awk '/^[\s]*UID_MIN/
{print $2}' /etc/login.defs)"') {print $1}' /etc/passwd | /usr/bin/xargs -I '{}' /usr/bin/passwd -
S '{}' | /usr/bin/awk '($2!="L" && $2!="LK") {print $1}' | /usr/bin/awk '{print} END {if (NR == 0)
 print "pass" ; else print "fail"}'' returned :

pass
```

5.4.3 Ensure default group for the root account is GID 0

Info

The usermod command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.

Rationale:

Using GID 0 for the root account helps prevent root -owned files from accidentally becoming accessible to non-privileged users.

Solution

Run the following command to set the root user default group to GID 0 :

usermod -g 0 root

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4

NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^root:x:0:0:

file: /etc/passwd regex: ^root:

system: Linux

Hosts

192.168.56.115

```
Compliant file(s):
      /etc/passwd - regex '^root:' found - expect '^root:x:0:0:' found in the following lines:
          1: root:x:0:0:root:/root:/bin/bash
```

5.4.4 Ensure default user umask is 027 or more restrictive - /etc/profile.d/*.sh

Info

The default umask determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile , .bashrc , etc.) in their home directories.

Rationale:

Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions. A default umask setting of 077 causes files and directories created by users to not be readable by any other user on the system. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

Solution

Edit the /etc/bash.bashrc, /etc/profile and /etc/profile.d/*.sh files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:

umask 027

Notes:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked.

Other methods of setting a default user umask exist however the shell configuration files are the last run and will override other settings if they exist therefor our recommendation is to configure in the shell configuration files. If other methods are in use in your environment they should be audited and the shell configs should be verified to not override.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4

CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*umask[\s]+[0-7][2-7]7[\s]*$ file: /etc/profile.d/*.sh regex: ^[\s]*umask[\s] required: NO system: Linux

Hosts

192.168.56.115

```
No matching files were found
```

5.5 Ensure root login is restricted to system console

Info

The file /etc/securetty contains a list of valid terminals that may be logged in directly as root.

Rationale:

Since the system console has special properties to handle emergency situations, it is important to ensure that the console is in a physically secure location and that unauthorized consoles have not been defined.

Solution

Remove entries for any consoles that are not in a physically secure location.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2(9)
800-53R5	AC-2(9)
CN-L3	8.1.4.2(c)
CSCV7	4.3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1NS
NIAV2	AM16
PCI-DSSV3.2.1	8.5
PCI-DSSV4.0	8.2.2
PCI-DSSV4.0	8.2.3
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: none system: Linux

Hosts

192.168.56.115

```
The command returned :

/bin/grep: /etc/securetty: No such file or directory
none
```

6.1.2 Ensure permissions on /etc/passwd are configured

Info

The /etc/passwd file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

Rationale:

It is critical to ensure that the /etc/passwd file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run the following command to set permissions on /etc/passwd:

chown root:root /etc/passwd # chmod 644 /etc/passwd

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
800-53R5	IA-5
800-53R5	IA-5(1)
CSCV6	3.1
CSCV7	16.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/passwd group: root mask: 133 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/passwd with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/passwd
```

6.1.3 Ensure permissions on /etc/gshadow- are configured

Info

The /etc/gshadow- file is used to store backup information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

It is critical to ensure that the /etc/gshadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run the one of the following chown commands as appropriate and the chmod to set permissions on /etc/gshadow- :

chown root:root /etc/gshadow- # chown root:shadow /etc/gshadow-

chmod o-rwx,g-wx /etc/gshadow-

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
800-53R5	IA-5
800-53R5	IA-5(1)
CSCV6	3.1
CSCV7	16.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/gshadow- group: root group: shadow mask: 137 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/gshadow- with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/gshadow-
```

6.1.4 Ensure permissions on /etc/shadow are configured

Info

The /etc/shadow file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert the user accounts.

Solution

Run the one following commands to set permissions on /etc/shadow:

chmod o-rwx,g-wx /etc/shadow

chown root:shadow /etc/shadow

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
800-53R5	IA-5
800-53R5	IA-5(1)
CSCV6	3.1
CSCV7	16.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/shadow group: shadow mask: 137 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/shadow with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/shadow
```

6.1.5 Ensure permissions on /etc/group are configured

Info

The /etc/group file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

Rationale:

The /etc/group file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Solution

Run the following command to set permissions on /etc/group:

chown root:root /etc/group

chmod 644 /etc/group

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
800-53R5	IA-5
800-53R5	IA-5(1)
CSCV6	3.1
CSCV7	16.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/group group: root mask: 133 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/group with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven permissions :
 FALSE is compliant with the policy value

/etc/group
```

6.1.6 Ensure permissions on /etc/passwd- are configured

Info

The /etc/passwd- file contains backup user account information.

Rationale:

It is critical to ensure that the /etc/passwd- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run the following command to set permissions on /etc/passwd- :

chown root:root /etc/passwd-

chmod u-x,go-rwx /etc/passwd-

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
800-53R5	IA-5
800-53R5	IA-5(1)
CSCV6	3.1
CSCV7	16.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/passwd- group: root mask: 133 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/passwd- with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/passwd-
```

6.1.7 Ensure permissions on /etc/shadow- are configured

Info

The /etc/shadow- file is used to store backup information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

It is critical to ensure that the /etc/shadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run the following commands to set permissions on /etc/shadow-:

chown root:shadow /etc/shadow-

chmod u-x,go-rwx /etc/shadow-

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
800-53R5	IA-5
800-53R5	IA-5(1)
CSCV6	3.1
CSCV7	16.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/shadow- group: root group: shadow mask: 137 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/shadow- with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/shadow-
```

6.1.8 Ensure permissions on /etc/group- are configured

Info

The /etc/group- file contains a backup list of all the valid groups defined in the system.

Rationale:

It is critical to ensure that the /etc/group- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run the following command to set permissions on /etc/group- :

chown root:root /etc/group-

chmod u-x,go-rwx /etc/group-

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
800-53R5	IA-5
800-53R5	IA-5(1)
CSCV6	3.1
CSCV7	16.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/group- group: root mask: 133 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/group- with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/group-
```

6.1.9 Ensure permissions on /etc/gshadow are configured

Info

The /etc/gshadow file is used to store the information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the /etc/gshadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/gshadow file (such as group administrators) could also be useful to subvert the group.

Solution

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

chown root:shadow /etc/gshadow

chmod o-rwx,g-wx /etc/gshadow

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
800-53R5	IA-5
800-53R5	IA-5(1)
CSCV6	3.1
CSCV7	16.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: /etc/gshadow group: root group: shadow mask: 137 owner: root system: Linux

Hosts

192.168.56.115

```
The file /etc/gshadow with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/gshadow
```

6.1.10 Ensure no world writable files exist

Info

Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the chmod(2) man page for more information.

Rationale:

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

Solution

Removing write access for the 'other' category (chmod o-w <filename>) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4

NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

name: find_world_writeable_files system: Linux

Hosts

192.168.56.115

```
No issues found.
```

6.1.11 Ensure no unowned files or directories exist

Info

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up 'owning' these files, and thus have more access on the system than was intended.

Solution

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.6
800-171	3.4.7
800-53	CM-7
800-53R5	CM-7
CSCV7	13.2
CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7
LEVEL	1S
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

find_option: nouser name: find_orphan_files system: Linux

Hosts

192.168.56.115

```
No issues found.
```

6.1.12 Ensure no ungrouped files or directories exist

Info

Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up 'owning' these files, and thus have more access on the system than was intended.

Solution

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.6
800-171	3.4.7
800-53	CM-7
800-53R5	CM-7
CSCV7	13.2
CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7
LEVEL	1S
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

find_option: nogroup name: find_orphan_files system: Linux

Hosts

192.168.56.115

```
No issues found.
```

6.2.1 Ensure password fields are not empty

Info

An account with an empty password field means that anybody may log in as that user without providing a password.

Rationale:

All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.

Solution

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it can be determined why it does not have a password:

passwd -l <username>

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be forced off.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/cat /etc/shadow | /usr/bin/awk -F : '($2 == "") { print $1 " does not have a password."}'| /usr/bin/awk '{print} END {if (NR == 0) print "none"'} expect: none system: Linux

Hosts

192.168.56.115

```
The command '/bin/cat /etc/shadow | /usr/bin/awk -F : '($2 == "") { print $1 " does not have a
 password."}'| /usr/bin/awk '{print} END {if (NR == 0) print "none"'}' returned :

none
```

6.2.2 Ensure no legacy '+' entries exist in /etc/passwd

Info

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Solution

Remove any legacy '+' entries from /etc/passwd if they exist.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.1
800-53	IA-2
800-53R5	IA-2
CN-L3	7.1.3.1(a)
CN-L3	7.1.3.1(e)
CN-L3	8.1.4.1(a)
CN-L3	8.1.4.2(a)
CN-L3	8.5.4.1(a)
CSCV7	16.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-2
ITSG-33	IA-2a.
LEVEL	1S
NESA	T2.3.8
NESA	T5.3.1
NESA	T5.4.2
NESA	T5.5.1
NESA	T5.5.2
NESA	T5.5.3

NIAV2	AM2
NIAV2	AM8
NIAV2	AM14b
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	35.1
TBA-FIISB	36.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*\+:

file: /etc/passwd regex: ^[\s]*\+:

system: Linux

Hosts

192.168.56.115

```
The file "/etc/passwd" does not contain "^[\s]*\+:"
```

6.2.3 Ensure all users' home directories exist

Info

Users can be defined in /etc/passwd without a home directory or with a home directory that does not actually exist.

Rationale:

If the user's home directory does not exist or is unassigned, the user will be placed in '/' and will not be able to write any files or have local environment variables set.

Solution

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

Notes:

The audit script checks all users with interactive shells except halt, sync, shutdown, and nfsnobody.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/cat /etc/passwd | /bin/egrep -v '^(root|halt|sync|shutdown)' | /usr/bin/awk -F: '($7 != "/usr/sbin/nologin" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do if [! -d "$dir"]; then /bin/echo

"The home directory ($dir) of user $user does not exist."; fi; done | /usr/bin/awk '{ print } END { if(NR==0) { print "No results found" } }'

expect: ^No results found$ system: Linux

Hosts

192.168.56.115

```
The command '/bin/cat /etc/passwd | /bin/egrep -v '^(root|halt|sync|shutdown)' | /usr/bin/awk -F:
 '($7 != "/usr/sbin/nologin" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do
 if [ ! -d "$dir" ]; then /bin/echo "The home directory ($dir) of user $user does not exist."; fi;
 done | /usr/bin/awk '{ print } END { if(NR==0) { print "No results found" } }'' returned :

No results found
```

6.2.4 Ensure no legacy '+' entries exist in /etc/shadow

Info

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Solution

Remove any legacy '+' entries from /etc/shadow if they exist.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.1
800-53	IA-2
800-53R5	IA-2
CN-L3	7.1.3.1(a)
CN-L3	7.1.3.1(e)
CN-L3	8.1.4.1(a)
CN-L3	8.1.4.2(a)
CN-L3	8.5.4.1(a)
CSCV6	16.9
CSCV7	16.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-2
ITSG-33	IA-2a.
LEVEL	1S
NESA	T2.3.8
NESA	T5.3.1
NESA	T5.4.2
NESA	T5.5.1
NESA	T5.5.2

NESA	T5.5.3
NIAV2	AM2
NIAV2	AM8
NIAV2	AM14b
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	35.1
TBA-FIISB	36.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*\+:

file: /etc/shadow regex: ^[\s]*\+:

system: Linux

Hosts

192.168.56.115

```
The file "/etc/shadow" does not contain "^[\s]*\+:"
```

6.2.5 Ensure no legacy '+' entries exist in /etc/group

Info

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Solution

Remove any legacy '+' entries from /etc/group if they exist.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.1
800-53	IA-2
800-53R5	IA-2
CN-L3	7.1.3.1(a)
CN-L3	7.1.3.1(e)
CN-L3	8.1.4.1(a)
CN-L3	8.1.4.2(a)
CN-L3	8.5.4.1(a)
CSCV7	16.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-2
ITSG-33	IA-2a.
LEVEL	1S
NESA	T2.3.8
NESA	T5.3.1
NESA	T5.4.2
NESA	T5.5.1
NESA	T5.5.2
NESA	T5.5.3

NIAV2	AM2
NIAV2	AM8
NIAV2	AM14b
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	35.1
TBA-FIISB	36.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

expect: ^[\s]*\+:

file: /etc/group regex: ^[\s]*\+:

system: Linux

Hosts

192.168.56.115

```
The file "/etc/group" does not contain "^[\s]*\+:"
```

6.2.6 Ensure root is the only UID 0 account

Info

Any account with UID 0 has superuser privileges on the system.

Rationale:

This access must be limited to only the default root account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 5.6 Ensure access to the su command is restricted.

Solution

Remove any users other than root with UID 0 or assign them a new UID if appropriate.

See Also

https://workbench.cisecurity.org/files/2658

References

800-53	SC-3
800-53R5	SC-3
CSCV6	5.1
CSCV7	4.6
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
LEVEL	1S
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

name: passwd_zero_uid system: Linux

Hosts

192.168.56.115

```
No issues found.
```

6.2.7 Ensure root PATH Integrity

Info

The root user can execute any command on the system and could be fooled into executing programs unintentionally if the PATH is not set correctly.

Rationale:

Including the current working directory (.) or other writable directory in root's executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as root to execute a Trojan horse program.

Solution

Correct or justify any items discovered in the Audit step.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	8.4
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: RPCV="$(sudo -Hiu root env | grep '^PATH' | cut -d= -f2)"; echo "$RPCV" | grep -q "::" && echo "root's path contains a empty directory (::)"; echo "$RPCV" | grep -q ":$" && echo "root's path contains a trailing (:)"; for x in $(echo "$RPCV" | tr ":" " "); do if [-d "$x"]; then ls -ldH "$x" | awk '$9 == "." {print "PATH contains current working directory (.)"}; $3 != "root" {print $9, "is not owned by root"}; substr($1,6,1) != "-" {print $9, "is group writable"}; substr($1,9,1) != "-" {print $9, "is world writable"}'; else echo "$x is not a directory"; fi; done | /usr/bin/awk '{print} END {if (NR == 0) print "All results passing"; else print "fail"}'

expect: All results passing system: Linux

Hosts

192.168.56.115

```
The command 'RPCV="$(sudo -Hiu root env | grep '^PATH' | cut -d= -f2)"; echo "$RPCV" | grep -q
 "::" && echo "root's path contains a empty directory (::)"; echo "$RPCV" | grep -q ":$" && echo
 "root's path contains a trailing (:)"; for x in $(echo "$RPCV" | tr ":" " "); do if [ -d "$x" ];
 then ls -ldH "$x" | awk '$9 == "." {print "PATH contains current working directory (.)"}; $3 !=
 "root" {print $9, "is not owned by root"}; substr($1,6,1) != "-" {print $9, "is group writable"};
 substr($1,9,1) != "-" {print $9, "is world writable"}'; else echo "$x is not a directory"; fi;
 done | /usr/bin/awk '{print} END {if (NR == 0) print "All results passing"; else print "fail"}''
 returned :

All results passing
```

6.2.8 Ensure users' home directories permissions are 750 or more restrictive

Info

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

Rationale:

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Solution

Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

Notes:

On some distributions the /sbin/nologin should be replaced with /usr/sbin/nologin.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3

LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: cat /etc/passwd | egrep -v '^(root|halt|sync|shutdown)' | awk -F: '($7 !~ "(/usr)?/sbin/nologin" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do if [! -d "$dir"]; then echo "The home directory ($dir) of user $user does not exist.";else dirperm=`ls -ld $dir | cut -f1 -d" "`;if [`echo $dirperm | cut -c6` != "-"]; then echo "Group Write permission set on the home directory ($dir) of user $user";fi;if [`echo $dirperm | cut -c8` != "-"]; then echo "Other Read permission set on the home directory ($dir) of user $user";fi;if [`echo $dirperm | cut -c9` != "-"]; then echo "Other Write permission set on the home directory ($dir) of user $user";fi;if [`echo $dirperm | cut -c10` != "-"]; then echo "Other Execute permission set on the home directory ($dir) of user $user";fi;fi;done | awk '{ print } END { if (NR==0) print "All home directories have proper permissions" }'

expect: All home directories have proper permissions system: Linux

Hosts

192.168.56.115

```
The command 'cat /etc/passwd | egrep -v '^(root|halt|sync|shutdown)' | awk -F: '($7 !~ "(/usr)?/
sbin/nologin" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do if [ ! -d
 "$dir" ]; then echo "The home directory ($dir) of user $user does not exist.";else dirperm=`ls -ld
 $dir | cut -f1 -d" "`;if [ `echo $dirperm | cut -c6` != "-" ]; then echo "Group Write permission
 set on the home directory ($dir) of user $user";fi;if [ `echo $dirperm | cut -c8` != "-" ]; then
 echo "Other Read permission set on the home directory ($dir) of user $user";fi;if [ `echo $dirperm
 | cut -c9` != "-" ]; then echo "Other Write permission set on the home directory ($dir) of user
 $user";fi;if [ `echo $dirperm | cut -c10` != "-" ]; then echo "Other Execute permission set on the
 home directory ($dir) of user $user";fi;fi;done | awk '{ print } END { if (NR==0) print "All home
 directories have proper permissions" }'' returned :

All home directories have proper permissions
```

6.2.9 Ensure users own their home directories

Info

The user home directory is space defined for the particular user to set local environment variables and to store personal files.

Rationale:

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

Solution

Change the ownership of any home directories that are not owned by the defined user to the correct user.

Notes:

On some distributions the /sbin/nologin should be replaced with /usr/sbin/nologin.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4

NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

name: accounts_bad_home_permissions system: Linux

Hosts

192.168.56.115

```
No issues found.
```

6.2.10 Ensure users' dot files are not group or world writable

Info

While the system administrator can establish secure permissions for users' 'dot' files, the users can easily override these.

Rationale:

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Solution

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.

Notes:

On some distributions the /sbin/nologin should be replaced with /usr/sbin/nologin.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S

NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: ~/.[!.]* mask: 022 system: Linux

Hosts

192.168.56.115

6.2.11 Ensure no users have .forward files

Info

The .forward file specifies an email address to forward the user's mail to.

Rationale:

Use of the .forward file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The .forward file also poses a risk as it can be used to execute commands that may perform unintended actions.

Solution

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

Notes:

On some distributions the /sbin/nologin should be replaced with /usr/sbin/nologin.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV6	9.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: ~/.forward system: Linux

Hosts

192.168.56.115

6.2.12 Ensure no users have .netrc files

Info

The .netrc file contains data for logging into a remote host for file transfers via FTP.

Rationale:

The .netrc file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over .netrc files from other systems which could pose a risk to those systems.

Solution

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

Notes:

On some distributions the /sbin/nologin should be replaced with /usr/sbin/nologin.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
800-53R5	IA-5
800-53R5	IA-5(1)
CSCV6	9.1
CSCV7	16.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

file: ~/.netrc system: Linux

Hosts

192.168.56.115

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

Info

While the system administrator can establish secure permissions for users' .netrc files, the users can easily override these.

Rationale:

.netrcfiles may contain unencrypted passwords that may be used to attack other systems.

Solution

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .netrc file permissions and determine the action to be taken in accordance with site policy.

Notes:

While the complete removal of .netrc files is recommended if any are required on the system secure permissions must be applied.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: for dir in $(/usr/bin/cat /etc/passwd | /usr/bin/egrep -v '(root|halt|sync|shutdown)' | /usr/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'); do if [-f "$dir/.netrc"]; then fileperm=$(ls -ld $dir/.netrc | cut -f1 -d" "); if [$(/usr/bin/echo $fileperm | cut -c5) != "-"]; then /usr/bin/echo "Group Read set on $dir/.netrc"; fi; if [$(/usr/bin/echo $fileperm | cut -c6) != "-"]; then /usr/bin/echo "Group Write set on $dir/.netrc"; fi; if [$(/usr/bin/echo $fileperm | cut -c7) != "-"]; then /usr/bin/echo "Group Execute set on $dir/.netrc"; fi; if [$(/usr/bin/echo $fileperm | cut -c8) != "-"]; then /usr/bin/echo "Other Read set on $dir/.netrc"; fi; if [$(/usr/bin/echo $fileperm | cut -c9) != "-"]; then /usr/bin/echo "Other Write set on $dir/.netrc"; fi; if [$(/usr/bin/echo $fileperm | cut -c10) != "-"]; then /usr/bin/echo "Other Execute set on $dir/.netrc"; fi; fi; done | /usr/bin/awk '{ print } END { if (NR==0) print "All .netrc files are not group or world accessible" }'

expect: All .netrc files are not group or world accessible system: Linux

Hosts

192.168.56.115

```
The command 'for dir in $(/usr/bin/cat /etc/passwd | /usr/bin/egrep -v '(root|halt|sync|shutdown)'
 | /usr/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'); do if [ -f "$dir/.netrc" ]; then
 fileperm=$(ls -ld $dir/.netrc | cut -f1 -d" "); if [ $(/usr/bin/echo $fileperm | cut -c5) != "-" ];
 then /usr/bin/echo "Group Read set on $dir/.netrc"; fi; if [ $(/usr/bin/echo $fileperm | cut -c6) !
= "-" ]; then /usr/bin/echo "Group Write set on $dir/.netrc"; fi; if [ $(/usr/bin/echo $fileperm |
 cut -c7) != "-" ]; then /usr/bin/echo "Group Execute set on $dir/.netrc"; fi; if [ $(/usr/bin/echo
 $fileperm | cut -c8) != "-" ]; then /usr/bin/echo "Other Read set on $dir/.netrc"; fi; if [ $(/
usr/bin/echo $fileperm | cut -c9) != "-" ]; then /usr/bin/echo "Other Write set on $dir/.netrc";
 fi; if [ $(/usr/bin/echo $fileperm | cut -c10) != "-" ]; then /usr/bin/echo "Other Execute set on
 $dir/.netrc"; fi; fi; done | /usr/bin/awk '{ print } END { if (NR==0) print "All .netrc files are
 not group or world accessible" }'' returned :

All .netrc files are not group or world accessible
```

6.2.14 Ensure no users have .rhosts files

Info

While no .rhosts files are shipped by default, users can easily create them.

Rationale:

This action is only meaningful if .rhosts support is permitted in the file /etc/pam.conf . Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf , they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

Solution

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .rhosts files and determine the action to be taken in accordance with site policy.

Notes:

On some distributions the /sbin/nologin should be replaced with /usr/sbin/nologin.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
800-53R5	IA-5
800-53R5	IA-5(1)
CSCV7	16.4
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /******* dont_echo_cmd: YES expect: No .rhosts files found system: Linux

Hosts

192.168.56.115

```
The command returned :

No .rhosts files found
```

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

Info

Over time, system administration errors and changes can lead to groups being defined in /etc/passwd but not in /etc/group .

Rationale:

Groups defined in the /etc/passwd file but not in the /etc/group file pose a threat to system security since group permissions are not properly managed.

Solution

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-171	3.5.5
800-171	3.5.6
800-53	AC-2
800-53	AC-2(3)
800-53	IA-4
800-53R5	AC-2
800-53R5	AC-2(3)
800-53R5	IA-4
CN-L3	7.1.2.7(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.2(e)
CN-L3	8.1.4.2(c)
CSCV7	16.6
CSCV7	16.7
CSCV7	16.8
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.9.2.6
ITSG-33	AC-2
ITSG-33	AC-2(3)
ITSG-33	IA-4
LEVEL	1S
NIAV2	AM26
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	5
TBA-FIISB	36.2.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

name: passwd_invalid_gid system: Linux

Hosts

192.168.56.115

```
No issues found.
```

6.2.16 Ensure no duplicate UIDs exist

Info

Although the useradd program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the /etc/passwd file and change the UID field.

Rationale:

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Solution

Based on the results of the audit script, establish unique UIDs and review all files owned by the shared UIDs to determine which UID they are supposed to belong to.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2
800-53R5	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

name: passwd_duplicate_uid system: Linux

Hosts

192.168.56.115

```
No duplicate User IDs detected
```

6.2.17 Ensure no duplicate GIDs exist

Info

Although the groupadd program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the /etc/group file and change the GID field.

Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

Solution

Based on the results of the audit script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

Notes:

You can also use the grpck command to check for other inconsistencies in the /etc/group file.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2
800-53R5	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1

QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

name: group_duplicate_gid system: Linux

Hosts

192.168.56.115

```
No duplicate Group IDs detected
```

6.2.18 Ensure no duplicate user names exist

Info

Although the useradd program will not let you create a duplicate user name, it is possible for an administrator to manually edit the /etc/passwd file and change the user name.

Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in /etc/passwd . For example, if 'test4' has a UID of 1000 and a subsequent 'test4' entry has a UID of 2000, logging in as 'test4' will use UID 1000. Effectively, the UID is shared, which is a security problem.

Solution

Based on the results of the audit script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2
800-53R5	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2

QCSC-V1 15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

name: passwd_duplicate_username system: Linux

Hosts

192.168.56.115

```
No issues found.
```

6.2.19 Ensure no duplicate group names exist

Info

Although the groupadd program will not let you create a duplicate group name, it is possible for an administrator to manually edit the /etc/group file and change the group name.

Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in /etc/group . Effectively, the GID is shared, which is a security problem.

Solution

Based on the results of the audit script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-2
800-53R5	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

name: group_duplicate_name system: Linux

Hosts

192.168.56.115

```
No issues found.
```

6.2.20 Ensure shadow group is empty

Info

The shadow group allows system programs which require access the ability to read the /etc/shadow file. No users should be assigned to the shadow group.

Rationale:

Any users assigned to the shadow group would be granted read access to the /etc/shadow file. If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert additional user accounts.

Solution

Remove all users from the shadow group, and change the primary group of any users with shadow as their primary group.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.1.1
800-53	AC-3
800-53R5	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5

NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/awk -F: 'FILENAME == "/etc/group" && $1 == "shadow" { gid=$3; if ($4!="") { print "secondary "$4; f=1 } } FILENAME == "/etc/passwd" && $4 == gid { print "primary "$1; f=1 } END { if (!f) print "shadow group empty" }' /etc/group /etc/passwd expect: ^shadow group empty$ system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/awk -F: 'FILENAME == "/etc/group" && $1 == "shadow" { gid=$3; if ($4!="")
 { print "secondary "$4; f=1 } } FILENAME == "/etc/passwd" && $4 == gid { print "primary "$1; f=1 }
 END { if (!f) print "shadow group empty" }' /etc/group /etc/passwd' returned :

shadow group empty
```

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit from CIS Debian Linux 10 Benchmark

See Also

https://workbench.cisecurity.org/files/2658

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.56.115

Compliance 'INFO', 'WARNING', 'ERROR'

1.2.1 Ensure package manager repositories are configured

Info

Systems need to have package manager repositories configured to ensure they receive the latest patches and updates.

Rationale:

If a system's package repositories are misconfigured important patches may not be identified or a rogue repository could introduce compromised software.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure your package manager repositories according to site policy.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.1
800-53	SI-2c.
800-53R5	SI-2c.
CN-L3	8.1.4.4(e)
CN-L3	8.1.10.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.5.4.1(b)
CN-L3	8.5.4.1(d)
CN-L3	8.5.4.1(e)
CSCV7	3.4
CSCV7	3.5
CSF	ID.RA-1
CSF	PR.IP-12
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-2
LEVEL	1NS
NESA	T7.6.2
NESA	T7.7.1
NIAV2	AM38
NIAV2	AM39

NIAV2	SS14b
PCI-DSSV3.2.1	6.2
PCI-DSSV4.0	6.3
PCI-DSSV4.0	6.3.3
QCSC-V1	11.2
SWIFT-CSCV1	2.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/apt-cache policy expect: system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/apt-cache policy' returned :

Package files:
 100 /var/lib/dpkg/status
     release a=now
 500 http://deb.debian.org/debian bookworm-updates/main amd64 Packages
     release v=12-updates,o=Debian,a=stable-updates,n=bookworm-updates,l=Debian,c=main,b=amd64
     origin deb.debian.org
 500 http://security.debian.org/debian-security bookworm-security/non-free-firmware amd64 Packages
     release v=12,o=Debian,a=stable-security,n=bookworm-security,l=Debian-Security,c=non-free-
firmware,b=amd64
     origin security.debian.org
 500 http://security.debian.org/debian-security bookworm-security/main amd64 Packages
     release v=12,o=Debian,a=stable-security,n=bookworm-security,l=Debian-Security,c=main,b=amd64
     origin security.debian.org
 500 http://deb.debian.org/debian bookworm/non-free-firmware amd64 Packages
     release v=12.1,o=Debian,a=stable,n=bookworm,l=Debian,c=non-free-firmware,b=amd64
     origin deb.debian.org
 500 http://deb.debian.org/debian bookworm/main amd64 Packages
     release v=12.1,o=Debian,a=stable,n=bookworm,l=Debian,c=main,b=amd64
     origin deb.debian.org
Pinned packages:
```

1.2.2 Ensure GPG keys are configured

Info

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

Rationale:

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

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

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

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.1
800-53	SI-2c.
800-53R5	SI-2c.
CN-L3	8.1.4.4(e)
CN-L3	8.1.10.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.5.4.1(b)
CN-L3	8.5.4.1(d)
CN-L3	8.5.4.1(e)
CSCV7	3.4
CSCV7	3.5
CSF	ID.RA-1
CSF	PR.IP-12
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-2
LEVEL	1NS
NESA	T7.6.2
NESA	T7.7.1
NIAV2	AM38
NIAV2	AM39
NIAV2	SS14b

PCI-DSSV3.2.1	6.2
PCI-DSSV4.0	6.3
PCI-DSSV4.0	6.3.3
QCSC-V1	11.2
SWIFT-CSCV1	2.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/apt-key list expect: system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/apt-key list' returned :

Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
/etc/apt/trusted.gpg.d/debian-archive-bookworm-automatic.asc
------------------------------------------------------------
pub   rsa4096 2023-01-21 [SC] [expires: 2031-01-19]
      B8B8 0B5B 623E AB6A D877  5C45 B7C5 D7D6 3509 47F8
uid           [ unknown] Debian Archive Automatic Signing Key (12/bookworm) <ftpmaster@debian.org>
sub   rsa4096 2023-01-21 [S] [expires: 2031-01-19]

/etc/apt/trusted.gpg.d/debian-archive-bookworm-security-automatic.asc
---------------------------------------------------------------------
pub   rsa4096 2023-01-21 [SC] [expires: 2031-01-19]
      05AB 9034 0C0C 5E79 7F44  A8C8 254C F3B5 AEC0 A8F0
uid           [ unknown] Debian Security Archive Automatic Signing Key (12/bookworm)
 <ftpmaster@debian.org>
sub   rsa4096 2023-01-21 [S] [expires: 2031-01-19]

/etc/apt/trusted.gpg.d/debian-archive-bookworm-stable.asc
---------------------------------------------------------
pub   ed25519 2023-01-23 [SC] [expires: 2031-01-21]
      4D64 FEC1 19C2 0290 67D6  E791 F8D2 585B 8783 D481
uid           [ unknown] Debian Stable Release Key (12/bookworm) <debian-release@lists.debian.org>

/etc/apt/trusted.gpg.d/debian-archive-bullseye-automatic.asc
------------------------------------------------------------
pub   rsa4096 2021-01-17 [SC] [expires: 2029-01-15]
      1F89 983E 0081 FDE0 18F3  CC96 73A4 F27B 8DD4 7936
uid           [ unknown] Debian Archive Automatic Signing Key (11/bullseye) <ftpmaster@debian.org>
sub   rsa4096 2021-01-17 [S] [expires: 2029-01-15]

/etc/apt/trusted.gpg.d/debian-archive-bullseye-security-automatic.asc
---------------------------------------------------------------------
pub   rsa4096 2021-01-17 [SC] [expires: 2029-01-15]
      AC53 0D52 0F2F 3269 F5E9  8313 A484 4904 4AAD 5C5D
uid           [ unknown] Debian Security Archive Automatic Signing Key (11/bullseye)
 <ftpmaster@debian.org>
sub   rsa4096 2021-01-17 [S] [expires: 2029-01-15 [...]
```

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

Info

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

Rationale:

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

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

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

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

apt upgrade OR # apt dist-upgrade

Notes:

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

upgrade: upgrade is used to install the newest versions of all packages currently installed on the system from the sources enumerated in /etc/apt/sources.list. Packages currently installed with new versions available are retrieved and upgraded; under no circumstances are currently installed packages removed, or packages not already installed retrieved and installed. New versions of currently installed packages that cannot be upgraded without changing the install status of another package will be left at their current version. An update must be performed first so that apt knows that new versions of packages are available.

dist-upgrade: dist-upgrade in addition to performing the function of upgrade, also intelligently handles changing dependencies with new versions of packages; apt has a 'smart' conflict resolution system, and it will attempt to upgrade the most important packages at the expense of less important ones if necessary. So, dist-upgrade command may remove some packages. The /etc/apt/sources.list file contains a list of locations from which to retrieve desired package files. See also apt_preferences(5) for a mechanism for overriding the general settings for individual packages.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.14.1
800-53	SI-2c.

800-53R5	SI-2c.
CN-L3	8.1.4.4(e)
CN-L3	8.1.10.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.5.4.1(b)
CN-L3	8.5.4.1(d)
CN-L3	8.5.4.1(e)
CSCV7	3.4
CSCV7	3.5
CSF	ID.RA-1
CSF	PR.IP-12
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-2
LEVEL	1NS
NESA	T7.6.2
NESA	T7.7.1
NIAV2	AM38
NIAV2	AM39
NIAV2	SS14b
PCI-DSSV3.2.1	6.2
PCI-DSSV4.0	6.3
PCI-DSSV4.0	6.3.3
QCSC-V1	11.2
SWIFT-CSCV1	2.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/apt-get -s upgrade expect: system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/apt-get -s upgrade' returned :

Reading package lists...
Building dependency tree...
Reading state information...
Calculating upgrade...
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

3.5.3.1 Ensure iptables are flushed - v4

Info

nftables is a replacement for iptables, ip6tables, ebtables and arptables

Rationale:

It is possible to mix iptables and nftables. However, this increases complexity and also the chance to introduce errors. For simplicity flush out all iptables rules, and ensure it is not loaded

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Run the following commands to flush iptables:

For iptables:

iptables -F

For ip6tables

ip6tables -F

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1NS
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d

NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/iptables -L expect: system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/iptables -L' returned :

bash: line 1: /usr/sbin/iptables: No such file or directory
```

3.5.3.1 Ensure iptables are flushed - v6

Info

nftables is a replacement for iptables, ip6tables, ebtables and arptables

Rationale:

It is possible to mix iptables and nftables. However, this increases complexity and also the chance to introduce errors. For simplicity flush out all iptables rules, and ensure it is not loaded

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Run the following commands to flush iptables:

For iptables:

iptables -F

For ip6tables

ip6tables -F

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1NS
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d

NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/sbin/iptables -L expect: system: Linux

Hosts

192.168.56.115

```
The command '/usr/sbin/iptables -L' returned :

bash: line 1: /usr/sbin/iptables: No such file or directory
```

3.5.3.8 Ensure nftables rules are permanent

Info

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/ datagrams/frames.

The nftables service reads the /etc/nftables.conf file for a nftables file or files to include in the nftables ruleset.

A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.

Rationale:

Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Edit the /etc/nftables.conf file and un-comment or add a line with include <Absolute path to nftables rules file> for each nftables file you want included in the nftables ruleset on boot example:

vi /etc/nftables.conf

Add the line:

include '/etc/nftables.rules'

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)

LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/cat /etc/nftables.conf expect: MANUAL_REVIEW system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/cat /etc/nftables.conf' returned :

#!/usr/sbin/nft -f

flush ruleset

table inet filter {
chain input {
type filter hook input priority filter;
}
chain forward {
type filter hook forward priority filter;
}
chain output {
type filter hook output priority filter;
}
}
```

3.5.4.2.3 Ensure IPv6 outbound and established connections are configured

Info

Configure the firewall rules for new outbound, and established IPv6 connections.

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT # ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT # ip6tables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT # ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT # ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT # ip6tables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV6	9.1
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)

ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1NS
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/ip6tables -L -v -n expect: system: Linux

Hosts

192.168.56.115

```
The command '/sbin/ip6tables -L -v -n' returned :

bash: line 1: /sbin/ip6tables: No such file or directory
```

3.5.4.2.4 Ensure IPv6 firewall rules exist for all open ports

Info

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

ip6tables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.13.1
800-53	SC-7(12)
800-53R5	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV6	9.1
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3

ITSG-33	SC-7(12)
LEVEL	1NS
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
PCI-DSSV3.2.1	1.4
PCI-DSSV4.0	1.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /usr/bin/ss -ln; /sbin/ip6tables -L INPUT -v -n expect: system: Linux

Hosts

192.168.56.115

```
The command '/usr/bin/ss -ln; /sbin/ip6tables -L INPUT -v -n' returned :

Netid   State    Recv-Q   Send-Q                                  Local Address:Port
              Peer Address:Port           Process
nl      UNCONN   0        0                                                0:1305
                          *
nl      UNCONN   0        0                                                0:1412
                          *
nl      UNCONN   0        0                                                0:498
                          *
nl      UNCONN   0        0                                                0:1720
                          *
nl      UNCONN   0        0                                                0:1599
                          *
nl      UNCONN   0        0                                                0:1304
                          *
nl      UNCONN   0        0                                                0:2776
                          *
nl      UNCONN   0        0                                                0:1338
                          *
nl      UNCONN   0        0                                                0:464
                          *
nl      UNCONN   0        0                                                0:1299
                          *
nl      UNCONN   0        0                                                0:0
                          *
nl      UNCONN   0        0                [...]
```

4.3 Ensure logrotate is configured

Info

The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file /etc/logrotate.d/rsyslog is the configuration file used to rotate log files created by rsyslog.

Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Edit /etc/logrotate.conf and /etc/logrotate.d/rsyslog to ensure logs are rotated according to site policy.

Notes:

If no maxage setting is set for logrotate a situation can occur where logrotate is interrupted and fails to delete rotated logfiles. It is recommended to set this to a value greater than the longest any log file should exist on your system to ensure that any such logfile is removed but standard rotation settings are not overridden.

See Also

https://workbench.cisecurity.org/files/2658

References

800-53	AU-4
800-53R5	AU-4
CSCV7	6.4
CSF	PR.DS-4
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-4
LEVEL	1NS
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

WARNING

Hosts

192.168.56.115

5.6 Ensure access to the su command is restricted

Info

The su command allows a user to run a command or shell as another user. The program has been superseded by sudo , which allows for more granular control over privileged access. Normally, the su command can be executed by any user. By uncommenting the pam_wheel.so statement in /etc/pam.d/su , the su command will only allow users in a specific groups to execute su. This group should be empty to reinforce the use of sudo for privileged access.

Rationale:

Restricting the use of su , and using sudo in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via sudo , whereas su can only record that a user executed the su program.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Create an empty group that will be specified for use of the su command. The group should be named according to site policy.

Example

groupadd sugroup

Add the following line to the /etc/pam.d/su file, specifying the empty group:

auth required pam_wheel.so use_uid group=sugroup

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep pam_wheel.so /etc/pam.d/su; /bin/cat /etc/group expect: Manual Review Required system: Linux

Hosts

192.168.56.115

```
The command '/bin/grep pam_wheel.so /etc/pam.d/su; /bin/cat /etc/group' returned :

# auth       required   pam_wheel.so
# auth       sufficient pam_wheel.so trust
# auth       required   pam_wheel.so deny group=nosu
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:
floppy:x:25:
tape:x:26:
sudo:x:27:
audio:x:29:
dip:x:30:
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:
staff:x:50:
games:x:60:
users:x:100:vboxuser
nogroup:x:65534:
systemd-journal:x:999:
systemd-network:x:998:
crontab:x:101:
input:x:102:
sgx:x:103:
kvm:x:104:
render:x:105:
netdev:x:106:
```

```
tss:x:107:
systemd-timesync:x:997:
messagebus:x:108:
_ssh:x:109:
ssl-cert:x:110:
avahi-autoipd:x:111:
bluetooth:x:112:
avahi:x:113:
lpadmin:x:114:
pipewire:x:115:
fwupd-refresh:x:116:
scanner:x:117:saned
saned:x:118:
geoclue:x:119:
polkitd:x:996:
rtkit:x:120:
colord:x:121:
Debian-gdm:x:122:
vboxuser:x:1000:
gnome-initial-setup:x:995:
```

6.1.13 Audit SUID executables

Info

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SUID programs, but it is important to identify and review such programs to ensure they are legitimate.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Ensure that no rogue SUID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1NS
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

name: find_suid_sgid_files system: Linux

Hosts

192.168.56.115

```
The following 26 files are SUID or SGID:

  /usr/lib/dbus-1.0/dbus-daemon-launch-helper
     owner: root, group: messagebus, permissions: 4754

  /usr/lib/openssh/ssh-keysign
     owner: root, group: root, permissions: 4755

  /usr/lib/polkit-1/polkit-agent-helper-1
     owner: root, group: root, permissions: 4755

  /usr/lib/xorg/Xorg.wrap
     owner: root, group: root, permissions: 6755

  /usr/libexec/camel-lock-helper-1.2
     owner: root, group: mail, permissions: 2755

  /usr/bin/pkexec
     owner: root, group: root, permissions: 4755

  /usr/bin/ssh-agent
     owner: root, group: _ssh, permissions: 2755

  /usr/bin/mount
     owner: root, group: root, permissions: 4755

  /usr/bin/umount
     owner: root, group: root, permissions: 4755

  /usr/bin/sudo
     owner: root, group: root, permissions: 4755

  /usr/bin/su
     owner: root, group: root, permissions: 4755

  /usr/bin/chfn
     owner: root, group: root, permissions: 4755

  /usr/bin/gpasswd
     owner: root, group: root, permissions: 4755

  /usr/bin/write
     owner: root, group: tty, permissions: 2755

  /usr/bin/expiry
     owner: root, group: shadow, permissions: 2755

  /usr/bin/dotlockfile
     owner: root, group: mail, permissions: 2755

  /usr/bin/wall
     owner: root, group: tty, permissions: 2755

  /usr/bin/passwd
     owner: root, group: root, permissions: 4755

  /usr/bin/crontab
     owner: root, group: crontab, permissions: 2755

  /usr/bin/newgrp
     owner: root, group: root, permissions: 4755

  /usr/bin/chsh
     owner: root, group: root, permissions: 4755
```

```
/usr/bin/fusermount3
   owner: root, group: root, permissions: 4755

/usr/bin/ntfs-3g
   owner: root, group: root, permissions: 4755

/usr/bin/chage
   owner: root, group: shadow, permissions: 2755

/usr/sbin/unix_chkpwd
   owner: root, group: shadow, permissions: 2755

/usr/sbin/pppd
   owner: root, group: dip, permissions: 4754
```

6.1.14 Audit SGID executables

Info

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different md5 checksum than what from the package. This is an indication that the binary may have been replaced.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Ensure that no rogue SGID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

See Also

https://workbench.cisecurity.org/files/2658

References

800-171	3.4.2
800-53	CM-6
800-53R5	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1NS
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_10_v1.0.0_L1_Server.audit

Policy Value

name: find_suid_sgid_files system: Linux

Hosts

192.168.56.115

```
The following 26 files are SUID or SGID:

  /usr/lib/dbus-1.0/dbus-daemon-launch-helper
     owner: root, group: messagebus, permissions: 4754

  /usr/lib/openssh/ssh-keysign
     owner: root, group: root, permissions: 4755

  /usr/lib/polkit-1/polkit-agent-helper-1
     owner: root, group: root, permissions: 4755

  /usr/lib/xorg/Xorg.wrap
     owner: root, group: root, permissions: 6755

  /usr/libexec/camel-lock-helper-1.2
     owner: root, group: mail, permissions: 2755

  /usr/bin/pkexec
     owner: root, group: root, permissions: 4755

  /usr/bin/ssh-agent
     owner: root, group: _ssh, permissions: 2755

  /usr/bin/mount
     owner: root, group: root, permissions: 4755

  /usr/bin/umount
     owner: root, group: root, permissions: 4755

  /usr/bin/sudo
     owner: root, group: root, permissions: 4755

  /usr/bin/su
     owner: root, group: root, permissions: 4755

  /usr/bin/chfn
     owner: root, group: root, permissions: 4755

  /usr/bin/gpasswd
     owner: root, group: root, permissions: 4755

  /usr/bin/write
     owner: root, group: tty, permissions: 2755

  /usr/bin/expiry
     owner: root, group: shadow, permissions: 2755

  /usr/bin/dotlockfile
     owner: root, group: mail, permissions: 2755

  /usr/bin/wall
     owner: root, group: tty, permissions: 2755

  /usr/bin/passwd
     owner: root, group: root, permissions: 4755

  /usr/bin/crontab
     owner: root, group: crontab, permissions: 2755

  /usr/bin/newgrp
     owner: root, group: root, permissions: 4755

  /usr/bin/chsh
     owner: root, group: root, permissions: 4755
```

```
/usr/bin/fusermount3
   owner: root, group: root, permissions: 4755

/usr/bin/ntfs-3g
   owner: root, group: root, permissions: 4755

/usr/bin/chage
   owner: root, group: shadow, permissions: 2755

/usr/sbin/unix_chkpwd
   owner: root, group: shadow, permissions: 2755

/usr/sbin/pppd
   owner: root, group: dip, permissions: 4754
```