



MF DEV CIS L1

Report generated by Tenable Nessus™

Wed, 25 Jun 2025 00:09:01 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.40.171.....13

Compliance 'FAILED'

- 1.6.2 Ensure local login warning banner is configured properly.....147
- 1.6.3 Ensure remote login warning banner is configured properly.....149
- 2.1.18 Ensure web server services are not in use.....151
- 4.2.4 Ensure ufw loopback traffic is configured.....153
- 4.2.7 Ensure ufw default deny firewall policy.....156
- 5.1.5 Ensure sshd Banner is configured.....159
- 5.1.20 Ensure sshd PermitRootLogin is disabled.....161
- 5.4.2.6 Ensure root user umask is configured.....163
- 5.4.3.3 Ensure default user umask is configured.....167
- 6.1.2.2 Ensure journald ForwardToSyslog is disabled.....173
- 6.1.3.6 Ensure rsyslog is configured to send logs to a remote log host.....176
- 6.1.4.1 Ensure access to all logfiles has been configured.....179
- 7.1.11 Ensure world writable files and directories are secured.....184
- 7.1.12 Ensure no files or directories without an owner and a group exist.....189

Compliance 'SKIPPED'

Compliance 'PASSED'

- 1.1.1.1 Ensure cramfs kernel module is not available.....194
- 1.1.1.2 Ensure freevxfs kernel module is not available.....197
- 1.1.1.3 Ensure hfs kernel module is not available.....200
- 1.1.1.4 Ensure hfsplus kernel module is not available.....203
- 1.1.1.5 Ensure jffs2 kernel module is not available.....206
- 1.1.1.9 Ensure usb-storage kernel module is not available.....209
- 1.1.2.1.1 Ensure /tmp is a separate partition.....212

• 1.1.2.1.2 Ensure nodev option set on /tmp partition.....	215
• 1.1.2.1.3 Ensure nosuid option set on /tmp partition.....	217
• 1.1.2.1.4 Ensure noexec option set on /tmp partition.....	220
• 1.1.2.2.1 Ensure /dev/shm is a separate partition.....	224
• 1.1.2.2.2 Ensure nodev option set on /dev/shm partition.....	226
• 1.1.2.2.3 Ensure nosuid option set on /dev/shm partition.....	230
• 1.1.2.2.4 Ensure noexec option set on /dev/shm partition.....	234
• 1.1.2.3.2 Ensure nodev option set on /home partition.....	238
• 1.1.2.3.3 Ensure nosuid option set on /home partition.....	241
• 1.1.2.4.2 Ensure nodev option set on /var partition.....	244
• 1.1.2.4.3 Ensure nosuid option set on /var partition.....	247
• 1.1.2.5.2 Ensure nodev option set on /var/tmp partition.....	250
• 1.1.2.5.3 Ensure nosuid option set on /var/tmp partition.....	253
• 1.1.2.5.4 Ensure noexec option set on /var/tmp partition.....	256
• 1.1.2.6.2 Ensure nodev option set on /var/log partition.....	259
• 1.1.2.6.3 Ensure nosuid option set on /var/log partition.....	262
• 1.1.2.6.4 Ensure noexec option set on /var/log partition.....	265
• 1.1.2.7.2 Ensure nodev option set on /var/log/audit partition.....	268
• 1.1.2.7.3 Ensure nosuid option set on /var/log/audit partition.....	271
• 1.1.2.7.4 Ensure noexec option set on /var/log/audit partition.....	274
• 1.2.2.1 Ensure updates, patches, and additional security software are installed.....	277
• 1.3.1.1 Ensure AppArmor is installed.....	280
• 1.3.1.2 Ensure AppArmor is enabled in the bootloader configuration.....	283
• 1.3.1.3 Ensure all AppArmor Profiles are in enforce or complain mode.....	287
• 1.4.1 Ensure bootloader password is set.....	291
• 1.4.2 Ensure access to bootloader config is configured.....	295
• 1.5.1 Ensure address space layout randomization is enabled.....	298
• 1.5.2 Ensure ptrace_scope is restricted.....	300
• 1.5.3 Ensure core dumps are restricted.....	303

• 1.5.4 Ensure prelink is not installed.....	306
• 1.5.5 Ensure Automatic Error Reporting is not enabled.....	309
• 1.6.1 Ensure message of the day is configured properly.....	311
• 1.6.4 Ensure access to /etc/motd is configured.....	313
• 1.6.5 Ensure access to /etc/issue is configured.....	316
• 1.6.6 Ensure access to /etc/issue.net is configured.....	319
• 1.7.2 Ensure GDM login banner is configured.....	322
• 1.7.3 Ensure GDM disable-user-list option is enabled.....	324
• 1.7.4 Ensure GDM screen locks when the user is idle.....	326
• 1.7.5 Ensure GDM screen locks cannot be overridden.....	329
• 1.7.6 Ensure GDM automatic mounting of removable media is disabled.....	332
• 1.7.7 Ensure GDM disabling automatic mounting of removable media is not overridden.....	334
• 1.7.8 Ensure GDM autorun-never is enabled.....	336
• 1.7.9 Ensure GDM autorun-never is not overridden.....	338
• 1.7.10 Ensure XDMCP is not enabled.....	340
• 2.1.1 Ensure autofs services are not in use.....	342
• 2.1.2 Ensure avahi daemon services are not in use.....	344
• 2.1.3 Ensure dhcp server services are not in use.....	346
• 2.1.4 Ensure dns server services are not in use.....	348
• 2.1.5 Ensure dnsmasq services are not in use.....	350
• 2.1.6 Ensure ftp server services are not in use.....	352
• 2.1.7 Ensure ldap server services are not in use.....	354
• 2.1.8 Ensure message access server services are not in use.....	356
• 2.1.9 Ensure network file system services are not in use.....	358
• 2.1.10 Ensure nis server services are not in use.....	360
• 2.1.11 Ensure print server services are not in use.....	362
• 2.1.12 Ensure rpcbind services are not in use.....	364
• 2.1.13 Ensure rsync services are not in use.....	366
• 2.1.14 Ensure samba file server services are not in use.....	368

• 2.1.15 Ensure snmp services are not in use.....	370
• 2.1.16 Ensure tftp server services are not in use.....	372
• 2.1.17 Ensure web proxy server services are not in use.....	374
• 2.1.19 Ensure xinetd services are not in use.....	376
• 2.1.21 Ensure mail transfer agent is configured for local-only mode.....	378
• 2.2.1 Ensure NIS Client is not installed.....	380
• 2.2.2 Ensure rsh client is not installed.....	382
• 2.2.3 Ensure talk client is not installed.....	384
• 2.2.4 Ensure telnet client is not installed.....	386
• 2.2.5 Ensure ldap client is not installed.....	388
• 2.2.6 Ensure ftp client is not installed.....	390
• 2.3.1.1 Ensure a single time synchronization daemon is in use.....	392
• 2.3.2.1 Ensure systemd-timesyncd configured with authorized timeserver.....	395
• 2.3.2.2 Ensure systemd-timesyncd is enabled and running.....	398
• 2.3.3.1 Ensure chrony is configured with authorized timeserver.....	400
• 2.3.3.2 Ensure chrony is running as user _chrony.....	403
• 2.3.3.3 Ensure chrony is enabled and running.....	405
• 2.4.1.1 Ensure cron daemon is enabled and active.....	407
• 2.4.1.2 Ensure permissions on /etc/crontab are configured.....	409
• 2.4.1.3 Ensure permissions on /etc/cron.hourly are configured.....	412
• 2.4.1.4 Ensure permissions on /etc/cron.daily are configured.....	415
• 2.4.1.5 Ensure permissions on /etc/cron.weekly are configured.....	418
• 2.4.1.6 Ensure permissions on /etc/cron.monthly are configured.....	421
• 2.4.1.7 Ensure permissions on /etc/cron.d are configured.....	424
• 2.4.1.8 Ensure crontab is restricted to authorized users.....	427
• 2.4.2.1 Ensure at is restricted to authorized users.....	431
• 3.1.2 Ensure wireless interfaces are disabled.....	435
• 3.1.3 Ensure bluetooth services are not in use.....	437
• 3.3.1 Ensure ip forwarding is disabled.....	439

• 3.3.2 Ensure packet redirect sending is disabled.....	442
• 3.3.3 Ensure bogus icmp responses are ignored.....	444
• 3.3.4 Ensure broadcast icmp requests are ignored.....	446
• 3.3.5 Ensure icmp redirects are not accepted.....	448
• 3.3.6 Ensure secure icmp redirects are not accepted.....	451
• 3.3.7 Ensure reverse path filtering is enabled.....	453
• 3.3.8 Ensure source routed packets are not accepted.....	455
• 3.3.9 Ensure suspicious packets are logged.....	458
• 3.3.10 Ensure tcp syn cookies is enabled.....	461
• 3.3.11 Ensure ipv6 router advertisements are not accepted.....	463
• 4.1.1 Ensure a single firewall configuration utility is in use.....	465
• 4.2.1 Ensure ufw is installed.....	468
• 4.2.2 Ensure iptables-persistent is not installed with ufw.....	471
• 4.2.3 Ensure ufw service is enabled.....	474
• 4.2.6 Ensure ufw firewall rules exist for all open ports.....	477
• 4.3.1 Ensure nftables is installed.....	480
• 4.3.2 Ensure ufw is uninstalled or disabled with nftables.....	483
• 4.3.3 Ensure iptables are flushed with nftables.....	486
• 4.3.4 Ensure a nftables table exists.....	489
• 4.3.5 Ensure nftables base chains exist.....	492
• 4.3.6 Ensure nftables loopback traffic is configured.....	495
• 4.3.7 Ensure nftables outbound and established connections are configured.....	498
• 4.3.8 Ensure nftables default deny firewall policy.....	501
• 4.3.9 Ensure nftables service is enabled.....	504
• 4.3.10 Ensure nftables rules are permanent.....	507
• 4.4.1.1 Ensure iptables packages are installed.....	510
• 4.4.1.2 Ensure nftables is not in use with iptables.....	513
• 4.4.1.3 Ensure ufw is not in use with iptables.....	516
• 4.4.2.1 Ensure iptables default deny firewall policy.....	519

• 4.4.2.2 Ensure iptables loopback traffic is configured.....	522
• 4.4.2.3 Ensure iptables outbound and established connections are configured.....	525
• 4.4.2.4 Ensure iptables firewall rules exist for all open ports.....	528
• 4.4.3.1 Ensure ip6tables default deny firewall policy.....	531
• 4.4.3.2 Ensure ip6tables loopback traffic is configured.....	534
• 4.4.3.3 Ensure ip6tables outbound and established connections are configured.....	537
• 4.4.3.4 Ensure ip6tables firewall rules exist for all open ports.....	540
• 5.1.1 Ensure permissions on /etc/ssh/sshd_config are configured.....	543
• 5.1.2 Ensure permissions on SSH private host key files are configured.....	547
• 5.1.3 Ensure permissions on SSH public host key files are configured.....	551
• 5.1.4 Ensure sshd access is configured.....	555
• 5.1.7 Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured.....	559
• 5.1.10 Ensure sshd HostbasedAuthentication is disabled.....	561
• 5.1.11 Ensure sshd IgnoreRhosts is enabled.....	563
• 5.1.12 Ensure sshd KexAlgorithms is configured.....	565
• 5.1.13 Ensure sshd LoginGraceTime is configured.....	569
• 5.1.14 Ensure sshd LogLevel is configured.....	571
• 5.1.15 Ensure sshd MACs are configured.....	574
• 5.1.16 Ensure sshd MaxAuthTries is configured.....	578
• 5.1.17 Ensure sshd MaxSessions is configured.....	581
• 5.1.18 Ensure sshd MaxStartups is configured.....	583
• 5.1.19 Ensure sshd PermitEmptyPasswords is disabled.....	585
• 5.1.21 Ensure sshd PermitUserEnvironment is disabled.....	587
• 5.1.22 Ensure sshd UsePAM is enabled.....	589
• 5.2.1 Ensure sudo is installed.....	591
• 5.2.2 Ensure sudo commands use pty.....	594
• 5.2.3 Ensure sudo log file exists.....	597
• 5.2.5 Ensure re-authentication for privilege escalation is not disabled globally.....	600
• 5.2.6 Ensure sudo authentication timeout is configured correctly.....	602

• 5.2.7 Ensure access to the su command is restricted.....	605
• 5.3.1.1 Ensure latest version of pam is installed.....	609
• 5.3.1.2 Ensure libpam-modules is installed.....	611
• 5.3.1.3 Ensure libpam-pwquality is installed.....	613
• 5.3.2.1 Ensure pam_unix module is enabled.....	615
• 5.3.2.2 Ensure pam_faillock module is enabled.....	619
• 5.3.2.3 Ensure pam_pwquality module is enabled.....	623
• 5.3.2.4 Ensure pam_pwhistory module is enabled.....	626
• 5.3.3.1.1 Ensure password failed attempts lockout is configured.....	629
• 5.3.3.1.2 Ensure password unlock time is configured.....	632
• 5.3.3.2.1 Ensure password number of changed characters is configured.....	635
• 5.3.3.2.2 Ensure minimum password length is configured.....	637
• 5.3.3.2.3 Ensure password complexity is configured.....	640
• 5.3.3.2.4 Ensure password same consecutive characters is configured.....	643
• 5.3.3.2.5 Ensure password maximum sequential characters is configured.....	645
• 5.3.3.2.6 Ensure password dictionary check is enabled.....	647
• 5.3.3.2.7 Ensure password quality checking is enforced.....	649
• 5.3.3.2.8 Ensure password quality is enforced for the root user.....	651
• 5.3.3.3.1 Ensure password history remember is configured.....	653
• 5.3.3.3.2 Ensure password history is enforced for the root user.....	655
• 5.3.3.3.3 Ensure pam_pwhistory includes use_authtok.....	657
• 5.3.3.4.1 Ensure pam_unix does not include nullok.....	660
• 5.3.3.4.2 Ensure pam_unix does not include remember.....	663
• 5.3.3.4.3 Ensure pam_unix includes a strong password hashing algorithm.....	665
• 5.3.3.4.4 Ensure pam_unix includes use_authtok.....	668
• 5.4.1.1 Ensure password expiration is configured.....	671
• 5.4.1.3 Ensure password expiration warning days is configured.....	674
• 5.4.1.4 Ensure strong password hashing algorithm is configured.....	678
• 5.4.1.5 Ensure inactive password lock is configured.....	681

• 5.4.1.6 Ensure all users last password change date is in the past.....	683
• 5.4.2.1 Ensure root is the only UID 0 account.....	685
• 5.4.2.2 Ensure root is the only GID 0 account.....	687
• 5.4.2.3 Ensure group root is the only GID 0 group.....	690
• 5.4.2.4 Ensure root account access is controlled.....	693
• 5.4.2.5 Ensure root path integrity.....	697
• 5.4.2.7 Ensure system accounts do not have a valid login shell.....	699
• 5.4.2.8 Ensure accounts without a valid login shell are locked.....	703
• 5.4.3.2 Ensure default user shell timeout is configured.....	707
• 6.1.1.1 Ensure journald service is enabled and active.....	711
• 6.1.1.2 Ensure journald log file access is configured.....	714
• 6.1.1.3 Ensure journald log file rotation is configured.....	718
• 6.1.1.4 Ensure only one logging system is in use.....	721
• 6.1.2.1.1 Ensure systemd-journal-remote is installed.....	723
• 6.1.2.1.2 Ensure systemd-journal-upload authentication is configured.....	726
• 6.1.2.1.3 Ensure systemd-journal-upload is enabled and active.....	729
• 6.1.2.1.4 Ensure systemd-journal-remote service is not in use.....	732
• 6.1.2.3 Ensure journald Compress is configured.....	734
• 6.1.2.4 Ensure journald Storage is configured.....	737
• 6.1.3.1 Ensure rsyslog is installed.....	740
• 6.1.3.2 Ensure rsyslog service is enabled and active.....	743
• 6.1.3.3 Ensure journald is configured to send logs to rsyslog.....	746
• 6.1.3.4 Ensure rsyslog log file creation mode is configured.....	750
• 6.3.1 Ensure AIDE is installed.....	755
• 6.3.2 Ensure filesystem integrity is regularly checked.....	758
• 7.1.1 Ensure permissions on /etc/passwd are configured.....	761
• 7.1.2 Ensure permissions on /etc/passwd- are configured.....	764
• 7.1.3 Ensure permissions on /etc/group are configured.....	767
• 7.1.4 Ensure permissions on /etc/group- are configured.....	770

• 7.1.5 Ensure permissions on /etc/shadow are configured.....	773
• 7.1.6 Ensure permissions on /etc/shadow- are configured.....	776
• 7.1.7 Ensure permissions on /etc/gshadow are configured.....	779
• 7.1.8 Ensure permissions on /etc/gshadow- are configured.....	782
• 7.1.9 Ensure permissions on /etc/shells are configured.....	785
• 7.1.10 Ensure permissions on /etc/security/opasswd are configured.....	788
• 7.2.1 Ensure accounts in /etc/passwd use shadowed passwords.....	792
• 7.2.2 Ensure /etc/shadow password fields are not empty.....	795
• 7.2.3 Ensure all groups in /etc/passwd exist in /etc/group.....	797
• 7.2.4 Ensure shadow group is empty.....	801
• 7.2.5 Ensure no duplicate UIDs exist.....	804
• 7.2.6 Ensure no duplicate GIDs exist.....	806
• 7.2.7 Ensure no duplicate user names exist.....	808
• 7.2.8 Ensure no duplicate group names exist.....	810
• 7.2.9 Ensure local interactive user home directories are configured.....	812
• 7.2.10 Ensure local interactive user dot files access is configured.....	816
• CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit from CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.....	821

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

• 1.1.1.10 Ensure unused filesystems kernel modules are not available.....	823
• 1.2.1.1 Ensure GPG keys are configured.....	827
• 1.2.1.2 Ensure package manager repositories are configured.....	830
• 2.1.22 Ensure only approved services are listening on a network interface.....	833
• 3.1.1 Ensure IPv6 status is identified.....	836
• 4.2.5 Ensure ufw outbound connections are configured.....	838
• 5.1.6 Ensure sshd Ciphers are configured.....	841
• 6.1.3.5 Ensure rsyslog logging is configured.....	845
• 6.1.3.7 Ensure rsyslog is not configured to receive logs from a remote client.....	848
• 6.1.3.8 Ensure logrotate is configured.....	850

• 7.1.13 Ensure SUID and SGID files are reviewed.....	853
---	-----

Remediations

• Suggested Remediations.....	858
-------------------------------	-----

Vulnerabilities by Host

192.168.40.171



Scan Information

Start time: Tue Jun 24 23:50:36 2025
End time: Wed Jun 25 00:08:58 2025

Host Information

IP: 192.168.40.171
MAC Address: BE:6D:7A:B5:1A:01 00:0C:29:C5:A8:D6 AE:2E:71:7F:77:6E 76:9D:56:10:84:65 1A:36:34:F3:64:23 CE:31:DB:5B:74:46 5A:AF:C3:5C:B3:9B 3E:7A:A5:3B:6D:CB F2:B4:1E:C8:F2:4B 62:6A:AF:31:0D:EB 8A:17:0D:D4:AF:BD
OS: Linux Kernel 6.8.0-60-generic on Ubuntu 24.04

Vulnerabilities

33851 - Network daemons not managed by the package system

Synopsis

Some daemon processes on the remote host are associated with programs that have been installed manually.

Description

Some daemon processes on the remote host are associated with programs that have been installed manually.

System administration best practice dictates that an operating system's native package management tools be used to manage software installation, updates, and removal whenever possible.

Solution

Use packages supplied by the operating system vendor whenever possible.

And make sure that manual software installation agrees with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2008/08/08, Modified: 2024/03/06

Plugin Output

tcp/0

```
The following running daemon is not managed by dpkg :
```

```
/var/www/ipo/go-ipo/app
```

34098 - BIOS Info (SSH)

Synopsis

BIOS info could be read.

Description

Using SMBIOS and UEFI, it was possible to get BIOS info.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2008/09/08, Modified: 2024/02/12

Plugin Output

tcp/0

```
Version      : 6.00
Vendor       : Phoenix Technologies LTD
Release Date : 11/12/2020
UUID        : 3a3a4d56-6171-109b-c91e-6b7ebcc5a8d6
Secure boot  : disabled
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Local checks have been enabled.
```


45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>

<https://nvd.nist.gov/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/04/15

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:canonical:ubuntu_linux:24.04.2::~esm~~ -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

cpe:/a:docker:docker:28.2.2 -> Docker
cpe:/a:gnupg:libgcrypt:1.10.3 -> GnuPG Libgcrypt
cpe:/a:google:protobuf:1.36.6 -> Google Protobuf
cpe:/a:haxx:curl:8.5.0 -> Haxx Curl
cpe:/a:haxx:libcurl:8.5.0 -> Haxx libcurl
cpe:/a:igor_sysoev:nginx:1.24.0 -> Nginx
cpe:/a:linuxfoundation:containerd:1.7.27 -> The Linux Foundation containerd
cpe:/a:mysql:mysql:8.0.42-0ubuntu0.24.04.1 -> MySQL MySQL
cpe:/a:mysql:mysql:8.0.42-0ubuntu0.24.04.1_ -> MySQL MySQL
cpe:/a:nginx:nginx:1.24.0 -> Nginx
cpe:/a:nginx:nginx:1.24.0-2 -> Nginx
cpe:/a:openbsd:openssh:9.6 -> OpenBSD OpenSSH

```
cpe:/a:openbsd:openssh:9.6p1 -> OpenBSD OpenSSH
cpe:/a:openssl:openssl:3.0.13 -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:7xongr -> OpenSSL Project OpenSSL
cpe:/a:oracle:openjdk:11.0.27 -> Oracle OpenJDK -
cpe:/a:php:php:8.1.32 -> PHP PHP
cpe:/a:tukaani:xz:5.6.1 -> Tukaani XZ
cpe:/a:vim:vim:9.1 -> Vim
cpe:/a:vmware:open_vm_tools:12.4.5 -> VMware Open VM Tools
x-cpe:/a:crowdstrike:falcon_sensor:7.25
x-cpe:/a:java:jre:11.0.27
```

237414 - Containerd Installed (Linux)

Synopsis

containerd was detected on the remote host.

Description

containerd, a container runtime which can manage the complete container lifecycle of its host system is installed on the target host.

See Also

<https://github.com/containerd/containerd/tree/main>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/05/28, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path           : /usr/bin/containerd
Version        : 1.7.27
Associated Package : containerd.io 1.7.27-1
Managed by OS  : True
```

165456 - CrowdStrike Falcon Sensor Installed (Linux)

Synopsis

CrowdStrike Falcon Sensor is installed on the remote Linux host.

Description

CrowdStrike Falcon Sensor, an agent for the Falcon platform, is installed on the remote Linux host.

See Also

<https://www.crowdstrike.com/endpoint-security-products/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/09/26, Modified: 2025/06/23

Plugin Output

tcp/0

```
Path      : /
Version   : 7.25
Agent ID  : 829345e9-f3f9-45b9-bela-2ba0fab09e35
Product   : CrowdStrike Falcon Sensor
Release   : 17804
Running   : 1
```

182774 - Curl Installed (Linux / Unix)

Synopsis

Curl is installed on the remote Linux / Unix host.

Description

Curl (also known as curl and cURL) is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://curl.se/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/09, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path          : /usr/bin/curl
Version       : 8.5.0
Associated Package : curl 8.5.0-2ubuntu10.6
Managed by OS : True
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/06/23

Plugin Output

tcp/0

```
Hostname : mfdev
mfdev (hostname command)
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 100
```

111529 - Docker Container Number of Changed Files

Synopsis

Checks for changes in running Docker containers and reports how many files changed.

Description

This plugin checks the docker diff information for each container and reports the number of changed files.

See Also

<https://www.docker.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/08/03, Modified: 2025/06/16

Plugin Output

tcp/0

```
Docker container 658c019d1369b99bbf42272d3e365f06d7188af4fc449363f50b885eff00f331 has 326721 changed files
Docker container 08e51112a9d7b55c77e44c1eebb6f352d0e97f7a2f9c7a3c54ab6a3256691f4f has 76 changed files
Docker container 9bbf6f880111f893b8e70a76e73bde846327bddf2facbcb2fb96c9041b212e14 has 34 changed files
Docker container 569a2079486d3f4be9dad8fd874a622b26058ecb066ca6159b1237e9bbf146fd has 74 changed files
Docker container 00f4a966f7b8bcc3b31e49487c6f87b772faec620996666cd49624e21ac13fe8 has 311178 changed files
Docker container 97013868077b455cecb05a33fa902df127b795bbb4cela62d628ffdc0b0f8cd has 313784 changed files
Docker container e465e783dfc5d7fe1ae59e55a448b8f7fd2958cf4ab72f5d075e2bf61da6b641 has 69 changed files
Docker container 989c4eec3d6f5506f7360f0354c479fcd116c8cf7ee90c48f77d10e4dcd820fb has 79 changed files
```


Docker container c8cab442fc07f8d33cb17432f0580e7bee4b25591b0c655fbf7d0191333169c8 has 34 changed files

159488 - Docker Installed (Linux)

Synopsis

Docker was detected on the remote host.

Description

A container virtualization suite is installed on the remote host.

See Also

<https://www.docker.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/04/04, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path      : /usr/bin/docker
Version   : 28.2.2
Build     : 45873be
Managed by OS : True
```

93561 - Docker Service Detection

Synopsis

Docker was detected on the remote host.

Description

The Docker service is running on the remote host. Docker is an open-source project that automates the deployment of applications inside software containers.

See Also

<https://www.docker.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/09/16, Modified: 2025/06/16

Plugin Output

tcp/0

```
Version: 28.2.2
Version: 28.2.2
Version: 1.7.27
Version: 1.2.5
Version: 0.19.0
```

The following containers were detected running on the remote Docker host :

```
Name:      /mailer
Image:      gauriab/rise-mailer
Image ID :  sha256:185c539211a9a226db88321c85f7bd9378552f6bdbf2dc8021a4469033c7be1f
Tag:        0.0.3-dev
ID:         658c019d1369b99bbf42272d3e365f06d7188af4fc449363f50b885eff00f331
Ports:      n/a
```

```
Name:      /admin
Image:      gauriab/rise-admin
Image ID :  sha256:9ebf3322f4dcce03abf529564c41d504143227b503ed8438649dd76741576cd2
Tag:        0.0.3-dev
ID:         08e51112a9d7b55c77e44cleebb6f352d0e97f7a2f9c7a3c54ab6a3256691f4f
Ports:      n/a
```

```
Name:      /redis
Image:      gauriab/rise-redis
```

```
Image ID : sha256:ed545ded7d620d0fd27973e4fcc7f9344fb32998201b70adcce524359b7b1a17
Tag:      0.0.3-dev
ID:       9bbf6f880111f893b8e70a76e73bde846327bddf2facbcb2fb96c9041b212e14
Ports:    n/a

Name:     /mstar
Image:    gauriab/rise-mstar
Image ID : sha256:d884ac82c55e7ccee3629ac712a917a44bc58df2f8611c098f022ad337c18d00
Tag:      0.0.3-dev
ID:       569a2079486d3f4be9dad8fd874a622b26058ecb066ca6159b1237e9bbf146fd
Ports:    n/a

Name:     /scheme
Image:    gauriab/rise-scheme
Image ID : sha256:d33ad0c69950edef9dc12ec93c7df22de7e6887d8002bcf25e8490ad2b5d073a
Tag:      0.0.3-dev
ID:       00f4a966f7b8bcc3b31e49487c6f87b772faec62099666cd49624e21ac13fe8
Ports:    n/a

Name:     /watchlist
Image:    gauriab/rise-watchlist
Image ID : sha256:9edf5a2aacfb4ed1be409d4c8241ce2a68fb5e30f4508ce7f575542fd65a4113
Tag:      0.0.3-dev
ID:       97013868077b455cecb05a33fa902df127b795bbb4ce1a62d628ffdc0b0f8cd
Ports:    n/a

Name:     /auth
Image:    gauriab/rise-auth
Image ID : sha256:a4bd6446581e1fef53f0fdebc8e73a3413b68daelf658f1c6e85d2298ef19eaa
Tag:      0.0.3-dev
ID:       e465e783dfc5d7felae59e55a448b8f7fd2958cf4ab72f5d075e2bf61da6b641
Ports:    n/a

Name:     /gateway
Image:    gauriab/rise-gateway
Image ID : sha256:5697d811fd410b36a3779b80499ebd90e70ceb456c963fb7b87653d02a475eab
Tag:      0.0.3-dev
ID [ ... ]
```

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

Plugin Output

tcp/0

The following IPv4 addresses are set on the remote host :

- 172.18.0.1 (on interface br-ef298930a6e8)
- 172.17.0.1 (on interface docker0)
- 192.168.40.171 (on interface ens160)
- 127.0.0.1 (on interface lo)

33276 - Enumerate MAC Addresses via SSH

Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

Published: 2008/06/30, Modified: 2022/12/20

Plugin Output

tcp/0

The following MAC addresses exist on the remote host :

- be:6d:7a:b5:1a:01 (interface vethcf0772e)
- 00:0c:29:c5:a8:d6 (interface ens160)
- ae:2e:71:7f:77:6e (interface veth244a458)
- 76:9d:56:10:84:65 (interface veth83c63bf)
- 1a:36:34:f3:64:23 (interface docker0)
- ce:31:db:5b:74:46 (interface br-ef298930a6e8)
- 5a:af:c3:5c:b3:9b (interface vethfd00865)
- 3e:7a:a5:3b:6d:cb (interface veth3761c96)
- f2:b4:1e:c8:f2:4b (interface veth573873a)
- 62:6a:af:31:0d:eb (interface vethd68f212)
- 8a:17:0d:d4:af:bd (interface veth7a129db)

170170 - Enumerate the Network Interface configuration via SSH

Synopsis

Nessus was able to parse the Network Interface data on the remote host.

Description

Nessus was able to parse the Network Interface data on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/01/19, Modified: 2025/02/11

Plugin Output

tcp/0

```
br-ef298930a6e8:
  MAC : ce:31:db:5b:74:46
  IPv4:
    - Address : 172.18.0.1
      Netmask : 255.255.0.0
      Broadcast : 172.18.255.255
veth3761c96:
  MAC : 3e:7a:a5:3b:6d:cb
vethd68f212:
  MAC : 62:6a:af:31:0d:eb
veth83c63bf:
  MAC : 76:9d:56:10:84:65
vethfd00865:
  MAC : 5a:af:c3:5c:b3:9b
veth573873a:
  MAC : f2:b4:1e:c8:f2:4b
veth7a129db:
  MAC : 8a:17:0d:d4:af:bd
veth244a458:
  MAC : ae:2e:71:7f:77:6e
ens160:
  MAC : 00:0c:29:c5:a8:d6
  IPv4:
    - Address : 192.168.40.171
      Netmask : 255.255.255.0
      Broadcast : 192.168.40.255
docker0:
  MAC : 1a:36:34:f3:64:23
  IPv4:
    - Address : 172.17.0.1
      Netmask : 255.255.0.0
      Broadcast : 172.17.255.255
```

```
lo:
  IPv4:
    - Address : 127.0.0.1
      Netmask : 255.0.0.0
vethcf0772e:
  MAC : be:6d:7a:b5:1a:01
```


179200 - Enumerate the Network Routing configuration via SSH

Synopsis

Nessus was able to retrieve network routing information from the remote host.

Description

Nessus was able to retrieve network routing information the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

Plugin Output

tcp/0

```
Gateway Routes:
  ens160:
    ipv4_gateways:
      192.168.40.5:
        subnets:
          - 0.0.0.0/0
Interface Routes:
  br-ef298930a6e8:
    ipv4_subnets:
      - 172.18.0.0/16
  docker0:
    ipv4_subnets:
      - 172.17.0.0/16
  ens160:
    ipv4_subnets:
      - 192.168.40.0/24
```

168980 - Enumerate the PATH Variables

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

Ensure that directories listed here are in line with corporate policy.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/06/23

Plugin Output

tcp/0

```
Nessus has enumerated the path of the current scan user :
```

```
/usr/local/sbin  
/usr/local/bin  
/usr/sbin  
/usr/bin  
/sbin  
/bin  
/usr/games  
/usr/local/games  
/snap/bin
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

<https://standards.ieee.org/faqs/regauth.html>

<http://www.nessus.org/u?794673b4>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

```
00:0C:29:C5:A8:D6 : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2025/06/10

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
- BE:6D:7A:B5:1A:01
- 00:0C:29:C5:A8:D6
- AE:2E:71:7F:77:6E
- 76:9D:56:10:84:65
- 1A:36:34:F3:64:23
- CE:31:DB:5B:74:46
- 5A:AF:C3:5C:B3:9B
- 3E:7A:A5:3B:6D:CB
- F2:B4:1E:C8:F2:4B
- 62:6A:AF:31:0D:EB
- 8A:17:0D:D4:AF:BD
```

168982 - Filepaths contain Dangerous characters (Linux)

Synopsis

This Tenable product detected files or paths on the scanned Unix-like system which contain characters with command injection or privilege escalation potential.

Description

This Tenable product detected files or paths on the scanned Unix-like system which contain characters with command injection or privilege escalation potential. Although almost any character is valid for an entry in this kind of filesystem, such as semicolons, use of some of them may lead to problems or security compromise when used in further commands.

This product has chosen in certain plugins to avoid digging within those files and directories for security reasons.

These should be renamed to avoid security compromise.

Solution

Rename these files or folders to not include dangerous characters.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The following files and directories contain potentially dangerous characters such as brackets,  
ampersand, or semicolon.
```

```
This scanner avoided access to these files when possible for safety:
```

```
/home/c3640/go/pkg/mod/github.com/gabriel-vasile/mimetype@v1.4.9/testdata/jar.jar  
/home/mf_dev/go/pkg/mod/github.com/gabriel-vasile/mimetype@v1.4.9/testdata/jar.jar
```

Synopsis

Google Protobuf module for Go is installed on the remote host

Description

Google Protobuf module for Go is installed on the remote host

See Also

<https://pkg.go.dev/google.golang.org/protobuf>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/04/12, Modified: 2025/06/16

Plugin Output

tcp/0

```
Nessus detected 2 installs of Google Protobuf:
```

```
Path      : /home/mf_dev/go/pkg/mod/google.golang.org/protobuf@v1.36.6/internal/version/version.go
Version   : 1.36.6
```

```
Path      : /home/c3640/go/pkg/mod/google.golang.org/protobuf@v1.36.6/internal/version/version.go
Version   : 1.36.6
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :  
nginx/1.24.0 (Ubuntu)
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK
```

```
Protocol version : HTTP/1.1
```

```
HTTP/2 TLS Support: No
```

```
HTTP/2 Cleartext Support: No
```

```
SSL : no
```

```
Keep-Alive : no
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
    Server: nginx/1.24.0 (Ubuntu)
```

```
    Date: Wed, 25 Jun 2025 03:54:02 GMT
```

```
    Content-Type: text/html
```

```
    Content-Length: 615
```

```
    Last-Modified: Sat, 03 May 2025 09:50:05 GMT
```

```
    Connection: keep-alive
```

```
    ETag: "6815e6cd-267"
```

```
    Accept-Ranges: bytes
```

```
Response Body :
```

```
<!DOCTYPE html>
```

```
<html>
```

```
<head>
```

```
<title>Welcome to nginx!</title>
```

```
<style>
```

```
html { color-scheme: light dark; }
```



```
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/5000/www

```
Response Code : HTTP/1.1 404 Not Found
```

```
Protocol version : HTTP/1.1
```

```
HTTP/2 TLS Support: No
```

```
HTTP/2 Cleartext Support: No
```

```
SSL : no
```

```
Keep-Alive : no
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
Content-Type: application/json; charset=utf-8
```

```
Date: Wed, 25 Jun 2025 03:54:02 GMT
```

```
Content-Length: 71
```

```
Connection: close
```

```
Response Body :
```

171410 - IP Assignment Method Detection

Synopsis

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/06/23

Plugin Output

tcp/0

```
+ lo
+ IPv4
  - Address      : 127.0.0.1
    Assign Method : static
+ ens160
+ IPv4
  - Address      : 192.168.40.171
    Assign Method : dynamic
+ docker0
+ IPv4
  - Address      : 172.17.0.1
    Assign Method : static
+ br-ef298930a6e8
+ IPv4
  - Address      : 172.18.0.1
    Assign Method : static
+ vethd68f212@if2
+ veth7a129db@if2
+ veth244a458@if2
+ veth83c63bf@if2
+ vethfd00865@if2
+ vethcf0772e@if2
+ veth3300dce@if2
+ veth8f6b2d7@if2
```

Synopsis

Java is installed on the remote Linux / Unix host.

Description

One or more instances of Java are installed on the remote Linux / Unix host. This may include private JREs bundled with the Java Development Kit (JDK).

Notes:

- This plugin attempts to detect Oracle and non-Oracle JRE instances such as Zulu Java, Amazon Corretto, AdoptOpenJDK, IBM Java, etc
- To discover instances of JRE that are not in PATH, or installed via a package manager, 'Perform thorough tests' setting must be enabled.

See Also

[https://en.wikipedia.org/wiki/Java_\(software_platform\)](https://en.wikipedia.org/wiki/Java_(software_platform))

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0690

Plugin Information

Published: 2021/03/16, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path          : /usr/lib/jvm/java-11-openjdk-amd64/
Version       : 11.0.27
Application    : OpenJDK Java
Binary Location : /usr/lib/jvm/java-11-openjdk-amd64/bin/java
Details        : This Java install appears to be OpenJDK due to the install directory
                  name (high confidence).
Detection Method : "find" utility
Managed by OS   : True
```

Note: readlink command was unable to be executed, because of this it is not possible to determine symlink java binaries. Duplicate instances may be reported.

151883 - Libgcrypt Installed (Linux/UNIX)

Synopsis

Libgcrypt is installed on this host.

Description

Libgcrypt, a cryptography library, was found on the remote host.

See Also

<https://gnupg.org/download/index.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2025/06/16

Plugin Output

tcp/0

```
Nessus detected 4 installs of Libgcrypt:

Path      : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.4.3
Version   : 1.10.3

Path      : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20
Version   : 1.10.3

Path      : /lib/x86_64-linux-gnu/libgcrypt.so.20.4.3
Version   : 1.10.3

Path      : /lib/x86_64-linux-gnu/libgcrypt.so.20
Version   : 1.10.3
```

Synopsis

Use system commands to obtain the list of mounted devices on the target machine at scan time.

Description

Report the mounted devices information on the target machine at scan time using the following commands.

```
/bin/df -h /bin/lsblk /bin/mount -l
```

This plugin only reports on the tools available on the system and omits any tool that did not return information when the command was ran.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/02/03, Modified: 2023/11/27

Plugin Output

tcp/0

```
$ df -h
Filesystem                                Size  Used Avail Use% Mounted on
tmpfs                                     2.4G  2.1M  2.4G   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv        265G   91G  161G  36% /
tmpfs                                     12G    0   12G   0% /dev/shm
tmpfs                                     5.0M    0   5.0M   0% /run/lock
tmpfs                                     4.0G   8.0K   4.0G   1% /tmp
/dev/sda2                                2.0G  192M   1.6G  11% /boot
overlay                                  265G   91G  161G  36% /var/lib/docker/
overlay2/125fbc6a267cad3cb52847eadf8751bbe8627a0c30ca9c8097681c3c255850a2/merged
overlay                                  265G   91G  161G  36% /var/lib/docker/overlay2/
fcb9b6e6dad4707b773a18798d18cf1735716718e07c76d5e0413ceecee06ac0/merged
overlay                                  265G   91G  161G  36% /var/lib/docker/
overlay2/83e5f77e5ed6f879c130dcba154cbea059ff2d72903df3a14978474dbd58d625/merged
overlay                                  265G   91G  161G  36% /var/lib/docker/
overlay2/5c55db1d901366a918afff3aca726dd1afef758abd9abb33bcb018e6d964deed/merged
overlay                                  265G   91G  161G  36% /var/lib/docker/
overlay2/61d768b18b987b8e7296840e3702b81616b410fca36294b07ab499ec6dd6c09b/merged
overlay                                  265G   91G  161G  36% /var/lib/docker/
overlay2/7fe1234be7eb91c51e87b4ad1d429bd60c8024e4074e3fddec1ba0de0e492fa/merged
overlay                                  265G   91G  161G  36% /var/lib/docker/overlay2/
fdd0e94eab6475979f8ca6df98befc566599c69b6eafa24b18a3568481ab8e4/merged
overlay                                  265G   91G  161G  36% /var/lib/docker/
overlay2/19db96d18950501ef80460e46778b242838c3b5b5d24df484bb3af6a95333f9d/merged
tmpfs                                     2.4G   16K   2.4G   1% /run/user/0
```

```
$ lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0                              7:0      0   11.5M  1 loop /snap/canonical-livepatch/316
loop1                              7:1      0   50.9M  1 loop /snap/snapd/24718
loop2                              7:2      0   63.8M  1 loop /snap/core20/25 [...]
```


193143 - Linux Time Zone Information

Synopsis

Nessus was able to collect and report time zone information from the remote host.

Description

Nessus was able to collect time zone information from the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2024/04/10, Modified: 2024/04/10

Plugin Output

tcp/0

```
Via date: IST +0530
Via timedatectl: Time zone: Asia/Kolkata (IST, +0530)
Via /etc/timezone: Asia/Kolkata
Via /etc/localtime: IST-5:30
```

95928 - Linux User List Enumeration

Synopsis

Nessus was able to enumerate local users and groups on the remote Linux host.

Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2025/03/26

Plugin Output

tcp/0

```
-----[ User Accounts ]-----
```

```
User       : nallen
Home folder : /home/nallen
Start script : /bin/bash
Groups      : lxd
              cdrom
              nallen
              plugdev
              dip
              adm
```

```
User       : cms
Home folder : /home/cms
Start script : /bin/bash
Groups      : cms
```

```
User       : c4197
Home folder : /home/c4197
Start script : /bin/bash
Groups      : mf_dev
              c4197
              docker
```

```
User       : mf_dev
Home folder : /home/mf_dev
Start script : /bin/bash
Groups      : mf_dev
              c3640
```

```

docker

User      : c3311
Home folder : /home/c3311
Start script : /bin/bash
Groups    : mf_dev
           users
           docker
           sudo
           c3311

User      : c4290
Home folder : /home/c4290
Start script : /bin/bash
Groups    : mf_dev
           users
           c4290
           docker

User      : c3640
Home folder : /home/c3640
Start script : /bin/bash
Groups    : c3640
           mf_dev
           users

User      : c4363
Home folder : /home/c4363
Start script : /bin/bash
Groups    : users
           c4363

-----[ System Accounts ]-----

User      : root
Home folder : /root
Start script : /bin/bash
Groups    : root
           docker

User      : daemon
Home folder : /usr/sbin
Start script : /usr/sbin/nologin
Groups    : daemon

User      : bin
Home folder : /bin
Start script : /usr/sbin/nologin
Groups    : bin

User      : sys
Home folder : /dev
Start script : /usr/sbin/nologin
Groups    : sys

User      : sync
Home folder : /bin
Start script : /bin/sync
Groups    : nogroup

User      : games
Home folder : /usr/games
Start script : /usr/sbin/nologin
Groups    : games

User      : man
Home folder : /var/cache/man
Start script : /usr/sbin/nologin
Groups    : man

```

```
User      : lp
Home folder : /var/spool/lpd
Start script : /usr/sbin/nologin
Groups     : lp

User      : [...]
```

45433 - Memory Information (via DMI)

Synopsis

Information about the remote system's memory devices can be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's memory devices, such as the total amount of installed memory.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/06, Modified: 2018/03/29

Plugin Output

tcp/0

```
Total memory : 24576 MB
```

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0802

Plugin Information

Published: 2001/08/13, Modified: 2022/10/12

Plugin Output

tcp/3306/mysql

```
Version : 8.0.42-0ubuntu0.24.04.1
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_PASSWORD (new more secure passwords)
  CLIENT_FOUND_ROWS (Found instead of affected rows)
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_NO_SCHEMA (Don't allow database.table.column)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_ODBC (ODBC client)
  CLIENT_LOCAL_FILES (Can use LOAD DATA LOCAL)
  CLIENT_IGNORE_SPACE (Ignore spaces before "(")
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_INTERACTIVE (This is an interactive client)
  CLIENT_SSL (Switch to SSL after handshake)
  CLIENT_SIGPIPE (IGNORE sigpipes)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_RESERVED (Old flag for 4.1 protocol)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

129468 - MySQL Server Installed (Linux)

Synopsis

MySQL Server is installed on the remote Linux host.

Description

MySQL Server is installed on the remote Linux host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/09/30, Modified: 2025/04/18

Plugin Output

tcp/0

```
Path      : /usr/sbin/mysqld
Version   : 8.0.42-0ubuntu0.24.04.1
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/06/06

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.8.4
Nessus build : 20028
Plugin feed version : 202506240723
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : es8-x86-64
Scan type : Normal
Scan name : MF DEV CIS L1
```



```
Scan policy used : Advanced Scan
Scanner IP : 192.168.40.34
Port scanner(s) : netstat
Port range : default
Ping RTT : 47.414 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'root' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/6/24 23:51 EDT (UTC -04:00)
Scan duration : 1074 sec
Scan for malware : no
```

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/68

```
Port 68/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/443/www

```
Port 443/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/514

```
Port 514/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/3306/mysql

```
Port 3306/tcp was found to be open
```


14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/5000/www

```
Port 5000/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/8181

```
Port 8181/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/8761

```
Port 8761/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/33060

```
Port 33060/tcp was found to be open
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : Ubuntu 16.04 Linux Kernel 4.4

Confidence level : 56

Method : MLSinFP

Type : unknown

Fingerprint : unknown

Remote operating system : Linux Kernel 6.8.0-60-generic

Confidence level : 99

Method : uname

Type : general-purpose

Fingerprint : uname:Linux mfdev 6.8.0-60-generic #63-Ubuntu SMP PREEMPT_DYNAMIC Tue Apr 15 19:04:15 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux

Remote operating system : Cisco Catalyst 9200 Series Switches

Cisco Catalyst 9300 Series Switches

Cisco Catalyst IE9300 Rugged Series

Nutanix

Confidence level : 59

Method : SinFP

Type :

Fingerprint : SinFP:

P1:B10113:F0x12:W64240:00204ffff:M1460:

P2:B10113:F0x12:W65160:00204ffff0402080affffff4445414401030307:M1460:

P3:B00000:F0x00:W0:00:M0

P4:191004_7_p=443

Remote operating system : Linux Kernel 6.8.0-60-generic on Ubuntu 24.04
Confidence level : 100
Method : LinuxDistribution
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :

SSH:!:SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.12
HTTP:!:Server: nginx/1.24.0 (Ubuntu)

SSLcert:!:i/CN:Go Daddy Secure Certificate Authority - G2i/O:GoDaddy.com, Inc.i/OU:http://
certs.godaddy.com/repository/s/CN:*.aliceblueonline.com
ea51929e61f33b80f22e897d5584b2df21648f05

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 6.8.0-60-generic on Ubuntu 24.04  
Confidence level : 100  
Method : LinuxDistribution
```

```
The remote host is running Linux Kernel 6.8.0-60-generic on Ubuntu 24.04
```

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

Synopsis

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

Plugin Output

tcp/0

```
It was possible to log into the remote host via SSH using 'keyboard-interactive' authentication.

The output of "uname -a" is :
Linux mfdev 6.8.0-60-generic #63-Ubuntu SMP PREEMPT_DYNAMIC Tue Apr 15 19:04:15 UTC 2025 x86_64
x86_64 x86_64 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
trixie/sid

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 4.569054 seconds
```


117887 - OS Security Patch Assessment Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0516

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
OS Security Patch Assessment is available.
```

```
Account : root
Protocol : SSH
```

148373 - OpenJDK Java Detection (Linux / Unix)

Synopsis

A distribution of Java is installed on the remote Linux / Unix host.

Description

One or more instances of OpenJDK Java are installed on the remote host. This may include private JREs bundled with the Java Development Kit (JDK).

Notes:

- Addition information provided in plugin Java Detection and Identification (Unix)
- Additional instances of Java may be discovered by enabling thorough tests

See Also

<https://openjdk.java.net/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/04/07, Modified: 2025/02/12

Plugin Output

tcp/0

```
Path          : /usr/lib/jvm/java-11-openjdk-amd64/
Version       : 11.0.27
Binary Location : /usr/lib/jvm/java-11-openjdk-amd64/bin/java
Managed by OS  : True
```

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

<https://www.openssh.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/06/16

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 9.6p1
Banner  : SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.12
```

168007 - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

The plugin timeout can be set to a custom value other than the plugin's default of 15 minutes via the 'timeout.168007' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

Note: This plugin leverages the '-maxdepth' find command option, which is a feature implemented by the GNU find binary. If the target does not support this option, such as HP-UX and AIX devices, users will need to enable 'thorough tests' in their scan policy to run the find command without using a '-maxdepth' argument.

See Also

<https://openssl.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/06/16

Plugin Output

tcp/0

Nessus detected 2 installs of OpenSSL:

Path	: /usr/lib/x86_64-linux-gnu/libcrypto.so.3
Version	: 7xongr
Associated Package	: libssl3t64
Path	: /usr/bin/openssl
Version	: 3.0.13
Associated Package	: openssl 3.0.13-0ubuntu3.5
Managed by OS	: True

We are unable to retrieve version info from the following list of OpenSSL files. However, these installs may include their version within the filename or the filename of the Associated Package.

e.g. libssl.so.3 (OpenSSL 3.x), libssl.so.1.1 (OpenSSL 1.1.x)

/usr/lib/x86_64-linux-gnu/libssl.so.3

216936 - PHP Scripting Language Installed (Unix)

Synopsis

The PHP scripting language is installed on the remote Unix host.

Description

The PHP scripting language is installed on the remote Unix host.

Note: Enabling the 'Perform thorough tests' setting will search the file system much more broadly.

Thorough test is required to get results on hosts running MacOS.

See Also

<https://www.php.net>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/13, Modified: 2025/06/16

Plugin Output

tcp/0

Nessus detected 3 installs of PHP:

Path	: /usr/lib/cgi-bin/php8.1
Version	: 8.1.32
Associated Package	: php8.1-cgi: /usr/lib/cgi-bin/php8.1
INI file	: /etc/php/8.1/cgi/php.ini
INI source	: PHP binary grep
Managed by OS	: True

Path	: /usr/bin/php8.1
Version	: 8.1.32
Associated Package	: php8.1-cli: /usr/bin/php8.1
INI file	: /etc/php/8.1/cli/php.ini
INI source	: PHP binary grep
Managed by OS	: True

Path	: /usr/bin/php-cgi8.1
Version	: 8.1.32
Associated Package	: php8.1-cgi: /usr/bin/php-cgi8.1
INI file	: /etc/php/8.1/cgi/php.ini

INI source	: PHP binary grep
Managed by OS	: True

179139 - Package Manager Packages Report (nix)

Synopsis

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/01, Modified: 2025/05/07

Plugin Output

tcp/0

Successfully retrieved and stored package data.

45432 - Processor Information (via DMI)

Synopsis

Nessus was able to read information about the remote system's processor.

Description

Nessus was able to retrieve information about the remote system's hardware, such as its processor type, by using the SMBIOS (aka DMI) interface.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/06, Modified: 2016/02/25

Plugin Output

tcp/0

Nessus detected 15 processors :

Current Speed : 2800 MHz
Version : Intel(R) Xeon(R) Platinum 8362 CPU @ 2.80GHz
Manufacturer : GenuineIntel
External Clock : Unknown
Status : Populated, Enabled
Family : Unknown
Type : Central Processor

Current Speed : 2800 MHz
Version : Intel(R) Xeon(R) Platinum 8362 CPU @ 2.80GHz
Manufacturer : GenuineIntel
External Clock : Unknown
Status : Populated, Enabled
Family : Unknown
Type : Central Processor

Current Speed : 2800 MHz
Version : Intel(R) Xeon(R) Platinum 8362 CPU @ 2.80GHz
Manufacturer : GenuineIntel
External Clock : Unknown
Status : Populated, Enabled
Family : Unknown
Type : Central Processor

Current Speed : 2800 MHz
Version : Intel(R) Xeon(R) Platinum 8362 CPU @ 2.80GHz
Manufacturer : GenuineIntel

```

External Clock : Unknown
Status         : Populated, Enabled
Family         : Unknown
Type           : Central Processor

Current Speed   : 2800 MHz
Version         : Intel(R) Xeon(R) Platinum 8362 CPU @ 2.80GHz
Manufacturer    : GenuineIntel
External Clock  : Unknown
Status         : Populated, Enabled
Family         : Unknown
Type           : Central Processor

Current Speed   : 2800 MHz
Version         : Intel(R) Xeon(R) Platinum 8362 CPU @ 2.80GHz
Manufacturer    : GenuineIntel
External Clock  : Unknown
Status         : Populated, Enabled
Family         : Unknown
Type           : Central Processor

Current Speed   : 2800 MHz
Version         : Intel(R) Xeon(R) Platinum 8362 CPU @ 2.80GHz
Manufacturer    : GenuineIntel
External Clock  : Unknown
Status         : Populated, Enabled
Family         : Unknown
Type           : Central Processor

Current Speed   : 2800 MHz
Version         : Intel(R) Xeon(R) Platinum 8362 CPU @ 2.80GHz
Manufacturer    : GenuineIntel
External Clock  : Unknown
Status         : Populated, Enabled
Family         : Unknown
Type           : Central Processor

Current Speed   : 2800 MHz
Version         : [...]

```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/22/ssh

```
Process ID      : 1
Executable     : /usr/lib/systemd/systemd
Command line   : /usr/lib/systemd/systemd --system --deserialize=83
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

udp/68

```
Process ID   : 2084963
Executable   : /usr/lib/systemd/systemd-networkd
Command line : /usr/lib/systemd/systemd-networkd
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/80/www

```
Process ID   : 2801209
Executable  : /usr/sbin/nginx
Command line : nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/443/www

```
Process ID   : 2801209
Executable  : /usr/sbin/nginx
Command line : nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/514

```
Process ID   : 943057
Executable  : /usr/sbin/rsyslogd
Command line : /usr/sbin/rsyslogd -n -iNONE
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/3306/mysql

```
Process ID   : 1973
Executable   : /usr/sbin/mysqld
Command line : /usr/sbin/mysqld
```


25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/5000/www

```
Process ID   : 3107143
Executable   : /var/www/ipo/go-ipo/app
Command line : /var/www/ipo/go-ipo/app
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/8181

```
Process ID   : 2828
Executable   : /usr/bin/docker-proxy
Command line : /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 8181 -container-ip
172.18.0.5 -container-port 8443 -use-listen-fd
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/8761

```
Process ID   : 2907
Executable   : /usr/bin/docker-proxy
Command line : /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 8761 -container-ip
172.18.0.6 -container-port 8761 -use-listen-fd
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/33060

```
Process ID   : 1973
Executable   : /usr/sbin/mysqld
Command line  : /usr/sbin/mysqld
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm(s) with the server :
```

```
Client to Server: aes256-ctr
Server to Client: aes256-ctr
```

```
The server supports the following options for compression_algorithms_server_to_client :
```

```
none
zlib@openssh.com
```

```
The server supports the following options for mac_algorithms_client_to_server :
```

```
hmac-sha1
hmac-sha2-256
hmac-sha2-512
umac-128@openssh.com
```

```
The server supports the following options for server_host_key_algorithms :
```

```
ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
```

```
The server supports the following options for encryption_algorithms_client_to_server :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
```

```
aes256-ctr
aes256-gcm@openssh.com
```

The server supports the following options for `mac_algorithms_server_to_client` :

```
hmac-sha1
hmac-sha2-256
hmac-sha2-512
umac-128@openssh.com
```

The server supports the following options for `kex_algorithms` :

```
curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
ext-info-s
kex-strict-s-v00@openssh.com
sntrup761x25519-sha512@openssh.com
```

The server supports the following options for `compression_algorithms_client_to_server` :

```
none
zlib@openssh.com
```

The server supports the following options for `encryption_algorithms_server_to_client` :

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

<https://tools.ietf.org/html/rfc4252#section-8>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :
```

- 1.99
- 2.0

Synopsis

The remote host supports the SCP protocol over SSH.

Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

See Also

https://en.wikipedia.org/wiki/Secure_copy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :
```

```
  hmac-sha1
```

```
The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :
```

```
  hmac-sha1
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.12
SSH supported authentication : publickey,password,keyboard-interactive
SSH banner :
All activities performed on this system will be monitored and reported.
Authorised users only.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/443/www

```
This port supports TLSv1.3/TLSv1.2.
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/443/www

The following soon to expire certificate was part of the certificate chain sent by the remote host :

```
| -Subject      : CN=*.aliceblueonline.com  
| -Not After   : Jul 31 11:09:24 2025 GMT
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

Purchase or generate a new SSL certificate in the near future to replace the existing one.

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/443/www

```
The SSL certificate will expire within 60 days, at  
Jul 31 11:09:24 2025 GMT :
```

```
Subject       : CN=*.aliceblueonline.com  
Issuer        : C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://  
certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2  
Not valid before : Jun 29 11:09:24 2024 GMT  
Not valid after  : Jul 31 11:09:24 2025 GMT
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
Subject Name:

Common Name: *.aliceblueonline.com

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: GoDaddy.com, Inc.
Organization Unit: http://certs.godaddy.com/repository/
Common Name: Go Daddy Secure Certificate Authority - G2

Serial Number: 29 9D 74 4D 91 B7 AB 01

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jun 29 11:09:24 2024 GMT
Not Valid After: Jul 31 11:09:24 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A6 3C 30 E1 72 F8 48 C4 AE D5 DF C3 EB B2 1D 9C FD 22 8A
             7D 32 4D 38 69 C8 4D 42 82 F5 C4 9A 60 F0 6A 39 EF 4C 57 17
             9A 6B D9 32 E6 0B FA B0 4E 71 25 EB C4 F3 CD 3A FF E5 C7 13
             CB 6E 93 3B 3F 77 C7 30 70 6E EB 71 72 89 6D A3 54 07 12 8E
             D2 3D 98 23 95 BB 3D 7C 69 41 B5 63 6E 0F D2 8A F4 37 13 2D
             FF C3 B9 11 7B EF 63 11 5E 28 A1 1A 57 B0 1D F9 7A 42 67 C1
```

```
69 D9 C0 CA AD 22 27 0B 76 CB 60 ED 66 94 AF A7 58 24 8C 2B
A5 BA E3 DE C8 19 1B E1 59 D5 B8 82 0E CD 5F 55 9D 15 E5 64
A4 F1 93 95 26 34 5F 5D 2D 80 42 B5 E3 E0 A2 3D 1A AF 73 33
90 DF 4D 5D 3F 98 2E F6 03 C2 2C DF 84 37 E0 88 DA 51 B8 61
D8 B0 BB A4 8F 5B 0B 9D 51 D8 B3 91 36 BC AE CE 9F 42 98 41
61 23 20 2C 2C 06 04 16 DD F3 91 4A 81 E6 93 33 33 58 21 75
95 F9 F9 11 3B BF BA A1 94 39 B9 A9 EA 66 78 F7 53
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 A9 04 0B 0A 4D 59 28 48 CA 22 DE 2A 66 38 8C DA 1E EB AB
37 9A EF CA 14 68 1E CB 53 2C FE E9 45 1F 58 FB C7 9F 32 05
F1 C6 80 04 32 ED DD 6D 1C 01 B8 B7 78 17 F5 B7 8C ED 14 E4
DC 68 55 71 49 F7 1E 97 88 CB 3C 84 FD D6 80 11 5F 95 A5 16
FA 8E A0 52 AE 28 86 68 4F 3C C8 7B EB CC C0 95 D0 05 1E 42
2F 17 DE A2 3F 33 87 CF E6 F6 8A 4B C0 92 3B A1 4C D4 0F DC
82 4E 7E 0B 23 65 67 29 B4 F1 CE C1 C8 5D A3 91 01 CD 3E 14
6B D8 91 [...]
```


95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

<http://www.nessus.org/u?ae636e78>

<https://tools.ietf.org/html/rfc3279>

<http://www.nessus.org/u?9bb87bf2>

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

tcp/443/www

```
Subject       : C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From    : Jun 29 17:06:20 2004 GMT
Valid To      : Jun 29 17:06:20 2034 GMT
```

-----BEGIN CERTIFICATE-----

MIIEADCCAuiGAWIBAgIBADANBgkqnkiG9w0BAQUFADBjMQswCQYDVQQGEWJVUzEhMB8GA1UEChMYVGVhIEdvIERhZGR5IEdyb3VwLCBjbMUMTEwLW
+vXX0iG6r7d/+TvZxz0ZWl3V3GgXne77ZtJ6XCAPVYYYwhv2vLMOD9/AlQiVB DYsoHUWHU9S3/
Hd8M+eKSA47UGay9qK7HFih7Eux6wwdhfJ2+qNlj3hybX2C32qr63H3I2TqYXP2WYktsqbl2i/
ojgc95/5Y0V4evLOtXiEQITLdiOrl8SPAIBQI2XKVlOARFMr6jYGB0xUGlcmIbYsUfb18aQr4CUWWorIMYavx4A6lNf4DD
+qta/KFApMoZFv6yyO9ecw3ud72a9nmYvLEHZ6IVDd2gWMZEewo+YihfukEHUl jPEX44dmX4/7VpkI
+EdOqXG68CAQOjgcAwgb0wHQYDVR0BBYEfnLEsNKRLewRcbNhzy2h/
t2oatTjMIGNBGnVHSMEgUYuwgYKAfnLEsNKRLewRcbNhzy2h/
t2oatTjoWeKztBJmQswCQYDVQQGEWJVUzEhMB8GA1UEChMYVGVhIEdvIERhZGR5IEdyb3VwLCBjbMUMTEwLWYDVQQLEyhHyBEYWRkeSBDbGFzcya
+YeAEW5p5JUXMP8OkWNyO07MHAGjHZQOPDH2esRUl/blmYgPoszoYtURXOl vOXJJLXvggKtI3lpjbi2Tc7PTMozI
+gciKqdi0FuFskg5YmezTvacPd+mSYgFFQl q25zheabIZ0KBIIoQPjCDPOQHmy74cNx A9hi63ugyuV+I6ShHI56yDgg
+2DzdzuCLzrTia2cyvk0/ZM/iZx4mERdEr/
VxqhD3VILs9RaRegAhJhldXRQLIQTO7ErBBdpqWeCTWVYPonZ4iCxTIM5CufReYNnyicsbkqwletNw+vHX/bvZ8=
-----END CERTIFICATE-----

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>

<http://www.nessus.org/u?cc4a822a>

<https://www.openssl.org/~bodo/tls-cbc.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/443/www

Here is the list of SSL CBC ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
ECDHE-RSA-CAMELLIA-CBC-128 SHA256	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)	
ECDHE-RSA-CAMELLIA-CBC-256 SHA384	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)	
ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	
AES128-SHA SHA1	0x00, 0x2F	RSA	RSA	AES-CBC(128)	

AES256-SHA SHA1	0x00, 0x35	RSA	RSA	AES-CBC(256)
CAMELLIA128-SHA SHA1	0x00, 0x41	RSA	RSA	Camellia-CBC(128)
CAMELLIA256-SHA SHA1	0x00, 0x84	RSA	RSA	Camellia-CBC(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)
RSA-AES128-SHA256 SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)
RSA-AES256-SHA256 SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)
RSA-CAMELLIA128-SHA256 SHA256	0x00, 0xBA	RSA	RSA	Camellia-CBC(128)
RSA-CAMELLIA256-SHA256 SHA256	0x00, 0xC0	RSA	RSA	Camellia-CBC(256)

The fields above are :

```

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>

<http://www.nessus.org/u?e17ffced>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/443/www

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv13

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
TLS_AES_128_GCM_SHA256	0x13, 0x01	-	-	AES-GCM(128)	
AEAD					
TLS_AES_256_GCM_SHA384	0x13, 0x02	-	-	AES-GCM(256)	
AEAD					
TLS_CHACHA20_POLY1305_SHA256	0x13, 0x03	-	-	ChaCha20-Poly1305(256)	
AEAD					

SSL Version : TLSv12

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
ECDHE-RSA-AES128-SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)	
SHA256					

ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)
ECDHE-RSA-CAMELLIA-CBC-128 SHA256	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)
ECDHE-RSA-CAMELLIA-CBC-256 SHA384	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)
ECDHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(256)
RSA-AES-128-CCM-AEAD AEAD	0xC0, 0x9C	RSA	RSA	AES-CCM(128)
RSA-AES-128-CCM8-AEAD AEAD	0xC0, 0xA0	RSA	RSA	AES-CCM8(128)
RSA-AES128-SHA256 SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)
RSA-AES-256-CCM-AEAD AEAD	0xC0, 0x9D	RSA	RSA	AES-CCM(256)
RSA-AES-256-CCM8-AEAD AEAD	0xC0, 0xA1	RSA	RSA	AES-CCM8(256)
RSA-AES256-SHA384	0x00, 0x9D	RSA	RSA	[...]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/443/www

Here is the list of SSL PFS ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
ECDHE-RSA-AES128-SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)	
SHA256					
ECDHE-RSA-AES256-SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)	
SHA384					
ECDHE-RSA-CAMELLIA-CBC-128	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)	
SHA256					
ECDHE-RSA-CAMELLIA-CBC-256	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)	
SHA384					
ECDHE-RSA-CHACHA20-POLY1305	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(256)	
SHA256					

ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)

The fields above are :

```

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

```


94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10))

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/443/www

The following root Certification Authority certificate was found :

```
| -Subject          : C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
| -Issuer          : C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
| -Valid From      : Jun 29 17:06:20 2004 GMT
| -Valid To       : Jun 29 17:06:20 2034 GMT
| -Signature Algorithm : SHA-1 With RSA Encryption
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

<https://ssl-config.mozilla.org/>

Solution

Only enable support for recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/443/www

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
ECDHE-RSA-CAMELLIA-CBC-128 SHA256	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)	
ECDHE-RSA-CAMELLIA-CBC-256 SHA384	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)	
RSA-AES-128-CCM-AEAD AEAD	0xC0, 0x9C	RSA	RSA	AES-CCM(128)	
RSA-AES-128-CCM8-AEAD AEAD	0xC0, 0xA0	RSA	RSA	AES-CCM8(128)	
RSA-AES128-SHA256 SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)	
RSA-AES-256-CCM-AEAD AEAD	0xC0, 0x9D	RSA	RSA	AES-CCM(256)	
RSA-AES-256-CCM8-AEAD AEAD	0xC0, 0xA1	RSA	RSA	AES-CCM8(256)	
RSA-AES256-SHA384 SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)	
ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	
AES128-SHA SHA1	0x00, 0x2F	RSA	RSA	AES-CBC(128)	
AES256-SHA SHA1	0x00, 0x35	RSA	RSA	AES-CBC(256)	
CAMELLIA128-SHA SHA1	0x00, 0x41	RSA	RSA	Camellia-CBC(128)	
CAMELLIA256-SHA SHA1	0x00, 0x84	RSA	RSA	Camellia-CBC(256)	
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)	
RSA-AES128-SHA256	0x00, 0x3C	RS [...]			

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/443/www

```
A TLSv1.2 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.2.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/5000/www

```
A web server is running on this port.
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2024/11/19

Plugin Output

tcp/3306/mysql

```
A MySQL server is running on this port.
```


22869 - Software Enumeration (SSH)

Synopsis

It was possible to enumerate installed software on the remote host via SSH.

Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, dpkg, etc.).

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0502

Plugin Information

Published: 2006/10/15, Modified: 2025/03/26

Plugin Output

tcp/0

Here is the list of packages installed on the remote Debian Linux system :

```
ii  acl 2.3.2-1build1.1 amd64 access control list - utilities
ii  adduser 3.137ubuntu1 all add and remove users and groups
ii  aide 0.18.6-2build2 amd64 Advanced Intrusion Detection Environment - dynamic binary
ii  aide-common 0.18.6-2build2 all Advanced Intrusion Detection Environment - Common files
ii  alsa-topology-conf 1.2.5.1-2 all ALSA topology configuration files
ii  alsa-ucm-conf 1.2.10-1ubuntu5.7 all ALSA Use Case Manager configuration files
ii  amd64-microcode 3.20250311.1ubuntu0.24.04.1 amd64 Processor microcode firmware for AMD
CPUs
ii  apparmor 4.0.1really4.0.1-0ubuntu0.24.04.4 amd64 user-space parser utility for AppArmor
ii  apparmor-utils 4.0.1really4.0.1-0ubuntu0.24.04.4 all utilities for controlling AppArmor
ii  appstream 1.0.2-1build6 amd64 Software component metadata management
ii  apt 2.8.3 amd64 commandline package manager
ii  apt-utils 2.8.3 amd64 package management related utility programs
ii  at-spi2-common 2.52.0-1build1 all Assistive Technology Service Provider Interface (common
files)
ii  at-spi2-core 2.52.0-1build1 amd64 Assistive Technology Service Provider Interface (D-Bus
core)
ii  base-files 13ubuntu10.2 amd64 Debian base system miscellaneous files
ii  base-passwd 3.6.3build1 amd64 Debian base system master password and group files
ii  bash 5.2.21-2ubuntu4 amd64 GNU Bourne Again SHell
```

```
ii  bash-completion 1:2.11-8 all programmable completion for the bash shell
ii  bc 1.07.1-3ubuntu4 amd64 GNU bc arbitrary precision calculator language
ii  bcache-tools 1.0.8-5build1 amd64 bcache userspace tools
ii  bind9-dnsutils 1:9.18.30-0ubuntu0.24.04.2 amd64 Clients provided with BIND 9
ii  bind9-host 1:9.18.30-0ubuntu0.24.04.2 amd64 DNS Lookup Utility
ii  bind9-libs 1:9.18.30-0ubuntu0.24.04.2 amd64 Shared Libraries used by BIND 9
ii  binutils 2.42-4ubuntu2.5 amd64 GNU assembler, [...]
```

35351 - System Information Enumeration (via DMI)

Synopsis

Information about the remote system's hardware can be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's hardware, such as its product name and serial number.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/01/12, Modified: 2025/03/18

Plugin Output

tcp/0

```
Chassis Information
  Serial Number : None
  Version       : N/A
  Manufacturer  : No Enclosure
  Lock          : Not Present
  Type          : Other

System Information
  Serial Number : VMware-56 4d 3a 3a 71 61 9b 10-c9 1e 6b 7e bc c5 a8 d6
  Version       : None
  Manufacturer  : VMware, Inc.
  Product Name  : VMware Virtual Platform
  Family        : Not Specified
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

<http://www.ietf.org/rfc/rfc1323.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

<https://tools.ietf.org/html/rfc7301>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2024/09/11

Plugin Output

tcp/443/www

```
http/1.1  
h2
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

<https://tools.ietf.org/html/rfc5246>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/443/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

<https://tools.ietf.org/html/rfc8446>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/443/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

110095 - Target Credential Issues by Authentication Protocol - No Issues Found

Synopsis

Nessus was able to log in to the remote host using the provided credentials. No issues were reported with access, privilege, or intermittent failure.

Description

Valid credentials were provided for an authentication protocol on the remote target and Nessus did not log any subsequent errors or failures for the authentication protocol.

When possible, Nessus tracks errors or failures related to otherwise valid credentials in order to highlight issues that may result in incomplete scan results or limited scan coverage. The types of issues that are tracked include errors that indicate that the account used for scanning did not have sufficient permissions for a particular check, intermittent protocol failures which are unexpected after the protocol has been negotiated successfully earlier in the scan, and intermittent authentication failures which are unexpected after a credential set has been accepted as valid earlier in the scan. This plugin reports when none of the above issues have been logged during the course of the scan for at least one authenticated protocol. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for issues to be encountered for one protocol and not another.

For example, authentication to the SSH service on the remote target may have consistently succeeded with no privilege errors encountered, while connections to the SMB service on the remote target may have failed intermittently.

- Resolving logged issues for all available authentication protocols may improve scan coverage, but the value of resolving each issue for a particular protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol and what particular check failed. For example, consistently successful checks via SSH are more critical for Linux targets than for Windows targets, and likewise consistently successful checks via SMB are more critical for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0520

Plugin Information

Published: 2018/05/24, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log into the remote host with no privilege or access  
problems via the following :
```

```
User:      'root'  
Port:      22  
Proto:     SSH  
Method:    keyboard-interactive
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.
- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

Nessus was able to log in to the remote host via the following :

```
User:      'root'
Port:      22
Proto:     SSH
Method:    keyboard-interactive
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

tcp/0

```
reboot    system boot 6.8.0-60-generic Mon Jun 16 17:30    still running
reboot    system boot 6.8.0-60-generic Mon Jun  2 09:18 - 17:29 (14+08:11)
reboot    system boot 6.8.0-59-generic Wed May 14 16:01 - 09:18 (18+17:16)
reboot    system boot 6.8.0-58-generic Fri May  2 11:08 - 16:00 (12+04:52)
reboot    system boot 6.8.0-58-generic Fri Apr 25 10:16 - 11:07 (7+00:51)
reboot    system boot 6.8.0-58-generic Thu Apr 24 11:30 - 10:16 (22:45)
reboot    system boot 6.8.0-58-generic Mon Apr 21 11:51 - 11:30 (2+23:38)
reboot    system boot 6.8.0-58-generic Mon Apr 21 11:19 - 11:51 (00:31)
reboot    system boot 6.8.0-58-generic Thu Apr 17 18:10 - 11:18 (3+17:08)
reboot    system boot 6.8.0-57-generic Thu Apr 17 15:08 - 18:10 (03:02)
reboot    system boot 6.8.0-57-generic Thu Apr 17 14:05 - 15:07 (01:02)
reboot    system boot 6.8.0-57-generic Thu Apr 17 12:50 - 14:05 (01:14)
reboot    system boot 6.8.0-57-generic Wed Apr 16 17:52 - 12:50 (18:57)
reboot    system boot 6.8.0-57-generic Wed Apr 16 15:51 - 17:30 (01:39)
reboot    system boot 6.8.0-57-generic Wed Apr 16 15:34 - 15:51 (00:17)
reboot    system boot 6.8.0-57-generic Wed Apr 16 12:55 - 15:34 (02:38)
reboot    system boot 6.8.0-57-generic Wed Apr 16 11:40 - 12:54 (01:14)
reboot    system boot 6.8.0-57-generic Tue Apr 15 18:24 - 11:40 (17:15)
reboot    system boot 6.8.0-57-generic Tue Apr 15 16:16 - 18:24 (02:08)
reboot    system boot 6.8.0-57-generic Mon Apr 14 13:03 - 16:15 (1+03:12)
reboot    system boot 6.8.0-57-generic Fri Apr 11 12:27 - 13:02 (3+00:35)
reboot    system boot 6.8.0-57-generic Fri Apr  4 10:17 - 12:26 (7+02:09)
reboot    system boot 6.8.0-57-generic Fri Apr  4 10:15 - 10:17 (00:01)
reboot    system boot 5.15.0-131-gener Fri Apr  4 05:42 - 10:14 (04:32)
reboot    system boot 5.15.0-131-gener Tue Apr  1 16:34 - 10:14 (2+17:40)
reboot    system boot 5.15.0-131-gener Sat Mar 29 19:03 - 16:34 (2+21:31)
reboot    system boot 5.15.0-131-gener Thu Mar 20 18:16 - 19:03 (9+00:46)
reboot    [...]
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.40.34 to 192.168.40.171 :  
192.168.40.34  
192.168.40.171
```

```
Hop Count: 1
```

192709 - Tukaani XZ Utils Installed (Linux / Unix)

Synopsis

Tukaani XZ Utils is installed on the remote Linux / Unix host.

Description

Tukaani XZ Utils is installed on the remote Linux / Unix host.

XZ Utils consists of several components, including:

- liblzma
- xz

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.192709' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://xz.tukaani.org/xz-utils/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2025/06/16

Plugin Output

tcp/0

Nessus detected 2 installs of XZ Utils:

Path	: /usr/bin/xz
Version	: 5.6.1
Associated Package	: xz-utils 5.6.1
Confidence	: High

```
Managed by OS      : True
Version Source     : Package

Path               : /usr/lib/x86_64-linux-gnu/liblzma.so.5.4.5
Version            : 5.6.1
Associated Package : liblzma5 5.6.1
Confidence         : High
Managed by OS     : True
Version Source     : Package
```

11765 - UPnP TCP Helper Detection

Synopsis

The remote host appears to be running Microsoft UPnP TCP helper.

Description

The remote host is running Microsoft UPnP TCP helper.

If the tested network is not a home network, you should disable this service.

Solution

Set the following registry key :

Location : HKLM\SYSTEM\CurrentControlSet\Services\SSDP\SRV Key : Start Value : 0x04

Risk Factor

None

Plugin Information

Published: 2003/06/19, Modified: 2019/11/22

Plugin Output

tcp/5000/www

198218 - Ubuntu Pro Subscription Detection

Synopsis

The remote Ubuntu host has an active Ubuntu Pro subscription.

Description

The remote Ubuntu host has an active Ubuntu Pro subscription.

See Also

<https://documentation.ubuntu.com/pro/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/05/31, Modified: 2024/07/05

Plugin Output

tcp/0

```
This machine is attached to an Ubuntu Pro subscription.
```

```
Subscription Contract Type : Ubuntu Pro + Infra Support (24/7)
Binary Path                : /var/lib/ubuntu-advantage
Binary Version             : 34~22.04
```

```
Enabled Ubuntu Pro Services :
- esm-apps
- esm-infra
- livepatch
```


110483 - Unix / Linux Running Processes Information

Synopsis

Uses `/bin/ps auxww` command to obtain the list of running processes on the target machine at scan time.

Description

Generated report details the running processes on the target machine at scan time.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

Plugin Output

tcp/0

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.0	23024	14336	?	Ss	Jun16	9:49	/usr/lib/systemd/systemd --system
--deserialize=83										
root	2	0.0	0.0	0	0	?	S	Jun16	0:02	[kthreadd]
root	3	0.0	0.0	0	0	?	S	Jun16	0:00	[pool_workqueue_release]
root	4	0.0	0.0	0	0	?	I<	Jun16	0:00	[kworker/R-rcu_g]
root	5	0.0	0.0	0	0	?	I<	Jun16	0:00	[kworker/R-rcu_p]
root	6	0.0	0.0	0	0	?	I<	Jun16	0:00	[kworker/R-slub_]
root	7	0.0	0.0	0	0	?	I<	Jun16	0:00	[kworker/R-netns]
root	9	0.0	0.0	0	0	?	I<	Jun16	0:00	[kworker/0:0H-events_highpri]
root	12	0.0	0.0	0	0	?	I<	Jun16	0:00	[kworker/R-mm_pe]
root	13	0.0	0.0	0	0	?	I	Jun16	0:00	[rcu_tasks_kthread]
root	14	0.0	0.0	0	0	?	I	Jun16	0:00	[rcu_tasks_rude_kthread]
root	15	0.0	0.0	0	0	?	I	Jun16	0:00	[rcu_tasks_trace_kthread]
root	16	0.0	0.0	0	0	?	S	Jun16	0:11	[ksoftirqd/0]
root	17	0.0	0.0	0	0	?	I	Jun16	3:27	[rcu_preempt]
root	18	0.0	0.0	0	0	?	S	Jun16	0:01	[migration/0]
root	19	0.0	0.0	0	0	?	S	Jun16	0:00	[idle_inject/0]
root	20	0.0	0.0	0	0	?	S	Jun16	0:00	[cpuhp/0]
root	21	0.0	0.0	0	0	?	S	Jun16	0:00	[cpuhp/1]
root	22	0.0	0.0	0	0	?	S	Jun16	0:00	[idle_inject/1]
root	23	0.0	0.0	0	0	?	S	Jun16	0:01	[migration/1]
root	24	0.0	0.0	0	0	?	S	Jun16	0:07	[ksoftirqd/1]
root	26	0.0	0.0	0	0	?	I<	Jun16	0:00	[kworker/1:0H-events_highpri]
root	27	0.0	0.0	0	0	?	S	Jun16	0:00	[cp [...]]

152742 - Unix Software Discovery Commands Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and is able to execute all commands used to find unmanaged software.

Description

Nessus was able to determine that it is possible for plugins to find and identify versions of software on the target host. Software that is not managed by the operating system is typically found and characterized using these commands. This was measured by running commands used by unmanaged software plugins and validating their output against expected results.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

Plugin Output

tcp/0

```
Unix software discovery checks are available.
```

```
Account   : root
Protocol  : SSH
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

Plugin Output

tcp/33060

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :
```

```
Port    : 33060
Type    : spontaneous
Banner  :
0x00:  05 00 00 00 0B 08 05 1A 00          .....
```

```
Nessus detected the following process listening on this port :
```

```
/usr/sbin/mysqld
```

186361 - VMWare Tools or Open VM Tools Installed (Linux)

Synopsis

VMWare Tools or Open VM Tools were detected on the remote Linux host.

Description

VMWare Tools or Open VM Tools were detected on the remote Linux host.

See Also

<https://kb.vmware.com/s/article/340>

<http://www.nessus.org/u?c0628155>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/11/28, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path      : /usr/bin/vmtoolsd
Version   : 12.4.5
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

189731 - Vim Installed (Linux)

Synopsis

Vim is installed on the remote Linux host.

Description

Vim is installed on the remote Linux host.

See Also

<https://www.vim.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/29, Modified: 2025/06/16

Plugin Output

tcp/0

```
Nessus detected 2 installs of Vim:
```

```
Path      : /usr/bin/vim.tiny
Version   : 9.1
```

```
Path      : /usr/bin/vim.basic
Version   : 9.1
```

182848 - libcurl Installed (Linux / Unix)

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://curl.se/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/06/16

Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:
```

```
Path           : /usr/lib/x86_64-linux-gnu/libcurl.so.4.8.0
Version        : 8.5.0
Associated Package : libcurl4t64

Path           : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.8.0
Version        : 8.5.0
Associated Package : libcurl3t64-gnutls
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL      : http://192.168.40.171/
Version  : 1.24.0
os       : Ubuntu
source   : Server: nginx/1.24.0 (Ubuntu)
```


136340 - nginx Installed (Linux/UNIX)

Synopsis

NGINX is installed on the remote Linux / Unix host.

Description

NGINX, a web server with load balancing capabilities, is installed on the remote Linux / Unix host.

See Also

<https://www.nginx.com>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/05/05, Modified: 2025/06/16

Plugin Output

tcp/0

Nessus detected 2 installs of nginx:

```
Path      : nginx (via package manager)
Version   : 1.24.0-2

Path      : /usr/sbin/nginx
Version   : 1.24.0
Associated Package : nginx: /usr/sbin/nginx
Detection Method  : Running Process
Full Version      : 1.24.0
Managed by OS    : True
Nginx Plus        : False
```

Compliance 'FAILED'

1.6.2 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

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

Example:

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.9
800-171R3	03.01.09
800-53	AC-8
800-53R5	AC-8
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-8
LEVEL	1A
NESA	M1.3.6
TBA-FIISB	45.2.4

Audit File

`CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit`

Policy Value

FAILED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

FAILED - Banner content

First ERROR: monitored and reported. != be monitored.

All activities performed on this system will be monitored and reported.

Authorised users only.

PASSED - mrsv not included in /etc/issue

The following file(s) do not contain "\\[mrsv]":

/etc/issue

1.6.3 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

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

Example:

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.9
800-171R3	03.01.09
800-53	AC-8
800-53R5	AC-8
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-8
LEVEL	1A
NESA	M1.3.6
TBA-FIISB	45.2.4

Audit File

`CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit`

Policy Value

FAILED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - mrsv not included in /etc/issue.net
The following file(s) do not contain "[mrsv]":
 /etc/issue.net

FAILED - banner text
First ERROR: monitored and reported. != be monitored.
All activities performed on this system will be monitored and reported.
Authorised users only.

2.1.18 Ensure web server services are not in use

Info

Web servers provide the ability to host web site content.

Unless there is a local site approved requirement to run a web server service on the system, web server packages should be removed to reduce the potential attack surface.

Solution

Run the following commands to stop httpd.socket httpd.service and nginx.service and remove apache2 and nginx packages:

```
# systemctl stop apache2.socket apache2.service nginx.service # apt purge apache2 nginx
```

- OR -

- IF - a package is installed and is required for dependencies:

Run the following commands to stop and mask apache2.socket apache2.service and nginx.service :

```
# systemctl stop apache2.socket apache2.service nginx.service # systemctl mask apache2.socket  
apache2.service nginx.service
```

Note: Other web server packages may exist. If not required and authorized by local site policy, they should also be removed. If the package is required for a dependency, the service and socket should be stopped and masked.

Impact:

Removal of web server packages will remove that ability for the server to host web services.

- IF - the web server package is required for a dependency, any related service or socket should be stopped and masked.

Note: If the remediation steps to mask a service are followed and that package is not installed on the system, the service and/or socket will still be masked. If the package is installed due to an approved requirement to host a web server, the associated service and/or socket would need to be unmasked before it could be enabled and/or started.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06

800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

FAILED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

 FAILED - is active

The command '/bin/systemctl is-active apache2.socket apache2.service nginx.service 2>/dev/null
 | /bin/grep '^active' | /bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}''
 returned :

active
 fail

 FAILED - is enabled

The command '/bin/systemctl is-enabled apache2.socket apache2.service nginx.service 2>/dev/null
 | /bin/grep 'enabled' | /bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}''
 returned :

enabled
 fail

4.2.4 Ensure ufw loopback traffic is configured

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).

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 configure the loopback interface to accept traffic:

```
# ufw allow in on lo # ufw allow out on lo
```

Run the following commands to configure all other interfaces to deny traffic to the loopback network:

```
# ufw deny in from 127.0.0.0/8 # ufw deny in from ::1
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5

CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

FAILED

Hosts

192.168.40.171

```
All of the following must pass to satisfy this requirement:

-----
FAILED - ufw - Anywhere DENY IN ::1
The command '/sbin/ufw status verbose' returned :

Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22/tcp ALLOW IN Anywhere
80/tcp ALLOW IN Anywhere
443/tcp ALLOW IN Anywhere
3306/tcp ALLOW IN Anywhere
33060/tcp ALLOW IN Anywhere
6379/tcp ALLOW IN 127.0.0.1
8443/tcp ALLOW IN Anywhere
8080/tcp ALLOW IN Anywhere
19532/tcp ALLOW IN Anywhere
8005/tcp ALLOW IN Anywhere
53/udp ALLOW IN Anywhere
68/udp ALLOW IN Anywhere
Anywhere on lo ALLOW IN Anywhere
Anywhere DENY IN 127.0.0.0/8
53 ALLOW IN Anywhere
8181 ALLOW IN Anywhere
8761 ALLOW IN Anywhere
25 ALLOW IN Anywhere
514/tcp ALLOW IN Anywhere
514/udp ALLOW IN Anywhere
5000 ALLOW IN Anywhere

Anywhere ALLOW OUT Anywhere on lo
Anywhere ALLOW OUT Anywhere on all

-----
PASSED - ufw - Anywhere DENY IN 127.0.0.0/8
The command '/sbin/ufw status verbose' returned :

Status: active
Logging: on (low)
Default [...]
```

4.2.7 Ensure ufw default deny firewall policy

Info

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

Note: Any port or protocol without a explicit allow before the default deny will be blocked

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

Impact:

Any port and protocol not explicitly allowed will be blocked. The following rules should be considered before applying the default deny.

```
ufw allow out http ufw allow out https ufw allow out ntp # Network Time Protocol ufw allow out to any port 53 # DNS ufw allow out to any port 853 # DNS over TLS ufw logging on
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4

CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /sbin/ufw status verbose | /bin/grep 'Default:'

expect: ^Default:[\s]+(deny|reject|disabled)[\s]+\(\(incoming\),[\s]+(deny|reject|disabled)[\s]+\(\(outgoing\),
[\s]+(deny|reject|disabled)[\s]+\(\(routed\)

Hosts

192.168.40.171

```
The command '/sbin/ufw status verbose | /bin/grep 'Default:'' returned :
```

```
Default: deny (incoming), allow (outgoing), disabled (routed)
```

5.1.5 Ensure sshd 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.

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 Banner parameter above any Include and Match entries as follows:

Banner `/etc/issue.net`

Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

Edit the file being called by the Banner argument with the appropriate contents according to your site policy, remove any instances of `m r s v` or references to the OS platform

Example:

```
# printf '%s ' "Authorized users only. All activity may be monitored and reported." > "$(sshd -T | awk '$1 == "banner" {print $2}')
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.9
800-171R3	03.01.09
800-53	AC-8
800-53R5	AC-8
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-8
LEVEL	1A
NESA	M1.3.6
TBA-FIISB	45.2.4

Audit File

Policy Value

FAILED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - Ensure banner is set to /etc/issue.net
The command script with multiple lines returned :

port 22: banner /etc/issue.net
Pass

PASSED - Ensure any instances of m, s, r, v or any references to the OS platform are removed from /
etc/issue.net
The command '/bin/grep -Psi -- "(\\v|\\r|\\m|\\s|\\b\$(/bin/grep '^ID=' /etc/os-release | /bin/cut
-d= -f2 | /bin/sed -e 's//g')\\b)" "\$(/sbin/sshd -T | /bin/awk '\$1 == "banner" {print \$2}')" | /
bin/awk '{ print } END { if(NR==0) print "Pass"; else print "Fail" }' returned :

Pass

FAILED - Ensure banner argument matches site policy
First ERROR: monitored and reported. != be monitored.
All activities performed on this system will be monitored and reported.
Authorised users only.

5.1.20 Ensure sshd PermitRootLogin is disabled

Info

The PermitRootLogin parameter specifies if the root user can log in using SSH. The default is prohibit-password

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

Solution

Edit the /etc/ssh/sshd_config file to set the PermitRootLogin parameter to no above any Include and Match entries as follows:

PermitRootLogin no

Note: First occurrence of an option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.5
800-171	3.1.6
800-171R3	03.01.06a.
800-171R3	03.01.06b.
800-53	AC-6(2)
800-53	AC-6(5)
800-53R5	AC-6(2)
800-53R5	AC-6(5)
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSCV7	4.3
CSCV8	5.4
CSF	PR.AC-4
CSF2.0	PR.AA-05
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	1A
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.6.1
NIAV2	AM1
NIAV2	AM23f
NIAV2	AM32
NIAV2	AM33
NIAV2	SS13c
NIAV2	SS15c
NIAV2	VL3a
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
SWIFT-CSCV1	1.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

```
The command script with multiple lines returned :

port 22: permitrootlogin yes
Fail
```

5.4.2.6 Ensure root user umask is configured

Info

The user file-creation mode mask (`umask`) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (`rw-rw-rw-`), and for any newly created file it is 0666 (`rw-rw-r--`). The `umask` modifies the default Linux permissions by restricting (masking) these permissions. The `umask` is not simply subtracted, but is processed bitwise. Bits set in the `umask` are cleared in the resulting file mode.

`umask` can be set with either Octal or Symbolic values:

- Octal (Numeric) Value - Represented by either three or four digits. ie `umask 0027` or `umask 027` If a four digit `umask` is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- Symbolic Value - Represented by a comma separated list for User `u` group `g` and world/other `o` The permissions listed are not masked by `umask` ie a `umask` set by `umask u=rwx,g=rx,o=` is the Symbolic equivalent of the Octal `umask 027` This `umask` would set a newly created directory with file mode `drwxr-x---` and a newly created file with file mode `rw-r-----`

root user Shell Configuration Files:

- `/root/.bash_profile` - Is executed to configure the root users' shell before the initial command prompt. Is only read by login shells.
- `/root/.bashrc` - Is executed for interactive shells. only read by a shell that's both interactive and non-login

`umask` is set by order of precedence. If `umask` is set in multiple locations, this order of precedence will determine the system's default `umask`

Order of precedence:

- `/root/.bash_profile`
- `/root/.bashrc`
- The system default `umask`

Setting a secure value for `umask` ensures that users make a conscious choice about their file permissions. A permissive `umask` value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

Solution

Edit `/root/.bash_profile` and `/root/.bashrc` and remove, comment out, or update any line with `umask` to be 0027 or more restrictive.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171 3.1.1

800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7

ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2

Audit File

CIS Ubuntu Linux 24.04 LTS v1.0.0 L1 Server.audit

Policy Value

```
expect: (?i)^\h*umask\h+(((0-7)[0-7][01][0-7]\b | 0-7[0-7][0-7][0-6]\b) | ((0-7)[01][0-7]\b | 0-7[0-7]
[0-6]\b) | (u=[rwx]{1,3},)?(((g=[rx]?[rx]?w[rx]?[rx]?[rb])(o=[rwx]{1,3}))? | ((g=[wrx]{1,3},)?o=[wrx]{1,3}\b))) file: /
root/.bash_profile /root/.bashrc regex: (?i)^\h*umask\h+(((0-7)[0-7][01][0-7]\b | 0-7[0-7][0-7][0-6]\b) | ((0-7)
[01][0-7]\b | 0-7[0-7][0-6]\b) | (u=[rwx]{1,3},)?(((g=[rx]?[rx]?w[rx]?[rx]?[rb])(o=[rwx]{1,3}))? | ((g=[wrx]{1,3},)?
o=[wrx]{1,3}\b)))
```

Hosts

192.168.40.171

```
Non-compliant file(s):  
    /root/.bashrc - regex '(?i)^\h*umask\h+([0-7][0-7][01][0-7]\b|[0-7][0-7][0-6]\b)|([0-7]  
[01][0-7]\b|[0-7][0-7][0-6]\b)|(u=[rxw]{1,3}),?(([g=rx]?[rx]?w[rx]?[rx]([,o=[rxw]{1,3})?)|  
((g=[rxw]{1,3}),)?o=[wxr]{1,3}\b))' found - expect '(?i)^\h*umask\h+([0-7][0-7][01][0-7]\b|[0-7]  
[0-7][0-7][0-6]\b)|([0-7][01][0-7]\b|[0-7][0-7][0-6]\b)|(u=[rxw]{1,3}),?(([g=rx]?[rx]?w[rx]?[rx]?  
\b)([,o=[rxw]{1,3})?)|((g=[wxr]{1,3}),)?o=[wxr]{1,3}\b)))' found in the following lines:  
101: umask 0022
```

5.4.3.3 Ensure default user umask is configured

Info

The user file-creation mode mask (`umask`) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (`rw-rw-rw-`), and for any newly created file it is 0666 (`rw-rw-r--`). The `umask` modifies the default Linux permissions by restricting (masking) these permissions. The `umask` is not simply subtracted, but is processed bitwise. Bits set in the `umask` are cleared in the resulting file mode.

`umask` can be set with either Octal or Symbolic values:

- Octal (Numeric) Value - Represented by either three or four digits. ie `umask 0027` or `umask 027` If a four digit `umask` is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- Symbolic Value - Represented by a comma separated list for User `u` group `g` and world/other `o` The permissions listed are not masked by `umask` ie a `umask` set by `umask u=rwx,g=rx,o=` is the Symbolic equivalent of the Octal `umask 027` This `umask` would set a newly created directory with file mode `drwxr-x---` and a newly created file with file mode `rw-r-----`

The default `umask` can be set to use the `pam_umask` module or in a System Wide Shell Configuration File The user creating the directories or files has the discretion of changing the permissions via the `chmod` command, or choosing a different default `umask` by adding the `umask` command into a User Shell Configuration File (`bash_profile` `orbashrc`), in their home directory.

Setting the default `umask`:

- `pam_umask` module:
 - will set the `umask` according to the system default in `/etc/login.defs` and user settings, solving the problem of different `umask` settings with different shells, display managers, remote sessions etc.
 - `umask=<mask>` value in the `/etc/login.defs` file is interpreted as Octal
 - Setting `USERGROUPS_ENAB` to `yes` in `/etc/login.defs` (default):
 - will enable setting of the `umask` group bits to be the same as owner bits. (examples: `022 -> 002`, `077 -> 007`) for non-root users, if the `uid` is the same as `gid` and `username` is the same as the `<primary group name>`
 - `userdel` will remove the user's group if it contains no more members, and `useradd` will create by default a group with the name of the user
- System Wide Shell Configuration File :
 - `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `bash_profile` however this file is used to set an initial `PATH` or `PS1` for all shell users of the system. is only executed for interactive

login

shells, or shells executed with the `--login` parameter.

- `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh` It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
- `/etc/bashrc` - System wide version of `bashrc` In Fedora derived distributions, `etc/bashrc` also invokes `/etc/profile.d/*.sh` if

non-login

shell, but redirects output to /dev/null if

non-interactive.

Is only executed for

interactive

shells or if BASH_ENV is set to /etc/bashrc

User Shell Configuration Files:

- ~/.bash_profile - Is executed to configure your shell before the initial command prompt. Is only read by login shells.

- ~/.bashrc - Is executed for interactive shells. only read by a shell that's both interactive and non-login

umask is set by order of precedence. If umask is set in multiple locations, this order of precedence will determine the system's default umask

Order of precedence:

- A file in /etc/profile.d/ ending insh - This will override any other system-wide umask setting

- In the file /etc/profile

- On the pam_umask.so module in /etc/pam.d/postlogin

- In the file /etc/login.defs

- In the file /etc/default/login

Setting a secure default value for umask ensures that users make a conscious choice about their file permissions. A permissive umask value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

Solution

Run the following script and perform the instructions in the output to set the default umask to 027 or more restrictive:

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

```
{ I_output="" I_output2="" I_out=""
```

```
file_umask_chk() { if grep -Psiq -- '^h*umaskh+(0?[0-7][2-7]7 | u(=[rwx]{0,3}),g=(=[rx]{0,2}),o=(h*#.*)?$',  
"$I_file"; then I_out="$I_out
```

```
- umask is set correctly in \"$I_file\"
```

```
elif grep -Psiq -- '^h*umaskh+(((0-7)[0-7][01][0-7]b | [0-7][0-7][0-7][0-6]b) | (([0-7][01][0-7]b | [0-7][0-7][0-6]b) |  
(u(=[rwx]{1,3}),)?(((g(=[rx]?[rx]?w[rx]?[rx]?b),o(=[rwx]{1,3})?) | ((g(=[rx]{1,3}),)?o(=[rwx]{1,3}b))))' "$I_file"; then  
I_output2="$I_output2
```

```
- \"$I_file\"
```

```
fi } while IFS= read -r -d $'0' I_file; do file_umask_chk done < <(find /etc/profile.d/ -type f -name '*.sh' -print0)  
[ -n "$I_out" ] && I_output="$I_out"
```

```
I_file="/etc/profile" && file_umask_chk I_file="/etc/bashrc" && file_umask_chk I_file="/etc/bash.bashrc" &&  
file_umask_chk I_file="/etc/pam.d/postlogin"
```



```

if grep -Psiq '^h*sessionh+[^# r]+h+pam_umask.soh+([^# r]+h+)?umask=(([0-7][0-7][01][0-7]b | [0-7][0-7][0-7][0-6]b) | ([0-7][01][0-7]b))' "$l_file"; then l_output2="$l_output2
- \"$l_file\"
fi l_file="/etc/login.defs" && file_umask_chk l_file="/etc/default/login" && file_umask_chk if [ -z
"$l_output2" ]; then echo -e " - No files contain a UMASK that is not restrictive enough No UMASK updates
required to existing files"
else echo -e "
- UMASK is not restrictive enough in the following file(s):$l_output2
- Remediation Procedure:
- Update these files and comment out the UMASK line or update umask to be \"0027\" or more restrictive"
fi if [ -n "$l_output" ]; then echo -e "$l_output"
else echo -e " - Configure UMASK in a file in the \"/etc/profile.d\" directory ending in \".sh\"

```

Example Command (Hash to represent being run at a root prompt):

```

# printf '%s\\ ' \"umask 027\" > /etc/profile.d/50-systemwide_umask.sh "
fi }

```

Notes:

- This method only applies to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked
- If the pam_umask.so module is going to be used to set umask ensure that it's not being overridden by another setting. Refer to the PAM_UMASK(8) man page for more information

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3

800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A

NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s***\s**pass:?\s***\\$

Hosts

192.168.40.171

The command script with multiple lines returned :

- Audit Result:

```
** FAIL **  
- * Reasons for audit failure * :  
  
- umask is incorrectly set in "/etc/login.defs"
```

6.1.2.2 Ensure journald ForwardToSyslog is disabled

Info

Data from journald should be kept in the confines of the service and not forwarded to other services.

- IF - journald is the method for capturing logs, all logs of the system should be handled by journald and not forwarded to other logging mechanisms.

Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

Solution

- IF - rsyslog is the preferred method for capturing logs, this section and Recommendation should be skipped and the "Configure rsyslog" section followed.

- IF - journald is the preferred method for capturing logs:

Set the following parameter in the [Journal] section in /etc/systemd/journald.conf or a file in /etc/systemd/journald.conf.d/ ending inconf :

ForwardToSyslog=no

Example script to create systemd drop-in configuration file:

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

```
{ a_settings=("ForwardToSyslog=no") [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir /etc/systemd/journald.conf.d/ if grep -Psq -- '^h*[Journal]' /etc/systemd/journald.conf.d/60-journald.conf; then printf '%s ' "${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf else printf '%s ' "" "[Journal]" "${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf fi }
```

Note: If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run to following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-2

800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.3
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s***\s**pass:?\s***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** FAIL **
- Reason(s) for audit failure:
  - Parameter: "ForwardToSyslog"
    incorrectly set to: "yes"
    in the file: "/usr/lib/systemd/journald.conf.d/syslog.conf"
    Should be set to: "no"
```

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

Info

rsyslog supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralized log management.

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 rsyslog configuration and add the following line (where loghost.example.com is the name of your central log host). The target directive may either be a fully qualified domain name or an IP address.

Example script to create a drop-in configuration file:

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

{ a_parameters=('*.* action(type="omfwd" target="loghost.example.com" port="514" protocol="tcp" '
action.resumeRetryCount="100" ' queue.type="LinkedList" queue.size="1000")) [ ! -d "/etc/rsyslog.d/" ] &&
mkdir /etc/rsyslog.d/ printf '%s ' "" "${a_parameters[@]}" >> /etc/rsyslog.d/60-rsyslog.conf }
```

Run the following command to reload rsyslog.service :

```
# systemctl reload-or-restart rsyslog.service
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2

CSCV7	6.3
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1M
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

FAILED

Hosts

192.168.40.171

One of the following must pass to satisfy this requirement:

FAILED - Ensure logs are sent to a central host - basic format
The command script with multiple lines did not return any result

FAILED - Ensure logs are sent to a central host - advanced format
The command script with multiple lines did not return any result

6.1.4.1 Ensure access to all logfiles has been configured

Info

Log files contain information from many services on the the local system, or in the event of a centralized log server, others systems logs as well.

In general log files are found in /var/log/ although application can be configured to store logs elsewhere. Should your application store logs in another, ensure to run the same test on that location.

It is important that log files have the correct permissions to ensure that sensitive data is protected and that only the appropriate users / groups have access to them.

Solution

Run the following script to update permissions and ownership on files in /var/log

Although the script is not destructive, ensure that the output of the audit procedure is captured in the event that the remediation causes issues.

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

```
{ a_output2=() f_file_test_fix() { a_out2=() maxperm="$( printf '%o' $(( 0777 & ~$perm_mask )) )"
if [ $(( $l_mode & $perm_mask )) -gt 0 ]; then a_out2+=(" o Mode: \"$l_mode\" should be \"$maxperm\" or
more restrictive" " x Removing excess permissions") chmod "$l_rperms" "$l_fname"
fi if [[ ! "$l_user" =~ $l_auser ]]; then a_out2+=(" o Owned by: \"$l_user\" and should be owned by
\"$l_auser//|/ or }\" " x Changing ownership to: \"$l_fix_account\") chown "$l_fix_account" "$l_fname"
fi if [[ ! "$l_group" =~ $l_agroup ]]; then a_out2+=(" o Group owned by: \"$l_group\" and should be
group owned by \"$l_agroup//|/ or }\" " x Changing group ownership to: \"$l_fix_account\") chgrp
"$l_fix_account" "$l_fname"
fi [ "${#a_out2[@]}" -gt 0 ] && a_output2+=(" - File: \"$l_fname\" is: " "${a_out2[@]}") } l_fix_account='root'
while IFS= read -r -d $'0' l_file; do while IFS=: read -r l_fname l_mode l_user l_group; do if grep -Pq -- '/
(apt)h*$' <<< "$(dirname "$l_fname")"; then perm_mask='0133' l_rperms="u-x,go-wx" l_auser="root"
l_agroup="(root|adm)"; f_file_test_fix else case "$(basename "$l_fname")" in lastlog | lastlog.* | wtmp
| wtmp.* | wtmp-* | bttmp | bttmp.* | bttmp-* | README) perm_mask='0113' l_rperms="ug-x,o-wx"
l_auser="root" l_agroup="(root|utmp)"
f_file_test_fix ;;
cloud-init.log* | localmessages* | waagent.log*) perm_mask='0133' l_rperms="u-x,go-wx" l_auser="(root|
syslog)" l_agroup="(root|adm)"
f_file_test_fix ;;
secure | auth.log | syslog | messages) perm_mask='0137' l_rperms="u-x,g-wx,o-rwx" l_auser="(root|
syslog)" l_agroup="(root|adm)"
f_file_test_fix ;;
SSSD | sssd) perm_mask='0117' l_rperms="ug-x,o-rwx" l_auser="(root|SSSD)" l_agroup="(root|SSSD)"
f_file_test_fix ;;
gdm | gdm3) perm_mask='0117' l_rperms="ug-x,o-rwx" l_auser="root" l_agroup="(root|gdm|gdm3)"
f_file_test_fix ;;
```

```

*.journal | *.journal~) perm_mask='0137' l_rperms="u-x,g-wx,o-rwx" l_auser="root" l_agroup="(root|
systemd-journal)"
f_file_test_fix ;;
*) perm_mask='0137' l_rperms="u-x,g-wx,o-rwx" l_auser="(root|syslog)" l_agroup="(root|adm)"
if [ "$l_user" = "root" ] || ! grep -Pq -- "^h*$(awk -F: ' $1==\"$l_user\" \" {print $7}' /etc/passwd)b" /etc/shells;
then ! grep -Pq -- "$l_auser" <<< "$l_user" && l_auser="(root|syslog|$l_user)"
! grep -Pq -- "$l_agroup" <<< "$l_group" && l_agroup="(root|adm|$l_group)"
fi f_file_test_fix ;;
esac fi done < <(stat -Lc '%n:%#a:%U:%G' "$l_file") done < <(find -L /var/log -type f ( -perm /0137 -o ! -user
root -o ! -group root ) -print0) if [ "${#a_output2[@]}" -le 0 ]; then # If all files passed, then we report no
changes a_output+="( " - All files in \" /var/log/ \" have appropriate permissions and ownership") printf '
%s' " - All files in \" /var/log/ \" have appropriate permissions and ownership" " o No changes required" ""
else printf '
%s' "${a_output2[@]}" ""
fi }

```

Note: You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.

If there are services that log to other locations, ensure that those log files have the appropriate permissions.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2

CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1

NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***[s]*pass:[s]***\$ timeout: 7200

Hosts

192.168.40.171

```
The command script with multiple lines returned :

/bin/bash: line 28: file_test_chk: command not found

/bin/bash: line 28: file_test_chk: command not found

- Audit Result:
```

```

** FAIL **
- Reason(s) for audit failure:
- File: "/var/log/ubuntu-advantage.log" is:
  o Mode: "0644" should be "640" or more restrictive
- File: "/var/log/dotfile_audit.log" is:
  o Mode: "0644" should be "640" or more restrictive
- File: "/var/log/btmp.1" is:
  o Group owned by: "adm" and should be group owned by "(root or utmp)"
- File: "/var/log/app.log" is:
  o Mode: "0644" should be "640" or more restrictive
- File: "/var/log/alternatives.log" is:
  o Mode: "0644" should be "640" or more restrictive
- File: "/var/log/journal/remote/remote-CN=*.aliceblueonline.com@0006319f75b0c10d-f3a029cd10907135.journal~" is:
  o Owned by: "systemd-journal-remote" and should be owned by "root"
- File: "/var/log/journal/remote/remote-192.168.40.33@deea0247ff274b8fbb204cd46cdef1cf-00000000002528bb-0006328321bcfe8d.journal" is:
  o Owned by: "systemd-journal-remote" and should be owned by "root"
- File: "/var/log/journal/remote/remote-CN=*.aliceblueonline.com@0006319fa698a078-41fca8b16e87b900.journal~" is:
  o Owned by: "systemd-journal-remote" and should be owned by "root"
- File: "/var/log/journal/remote/remote-192.168.40.33@deea0247ff274b8fbb204cd46cdef1cf-0000000000000001-000631b1abc37576.journal" is:
  o Owned by: "systemd-journal-remote" and should be owned by "root"
- File: "/var/log/journal/remote/remote-CN=*.aliceblueonline.com@0006319fc0da21bb-76e2f07b3647ba8d.journal~" is:
  o Owned by: "systemd-journal-remote" and should be owned by "root"
- File: "/var/log/journal/remote/remote-192.168.40.31@29e7764d42294f958f906f3b207102e5-000000000000cae90-000632b5c49bfa19.journal" is:
  o Owned by: "systemd-journal-remote" and should be owned by "root"
- File: "/var/log/journal/remote/remote-192.168.40.33@deea0247ff274b8fbb204cd46cdef1cf-00000000003188f9-000632cf8a91da3f.journal" is:
  o Owned by: "systemd-journal-remote" and sh [...]

```

7.1.11 Ensure world writable files and directories are secured

Info

World writable files are the least secure. Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity. See the `chmod(2)` man page for more information.

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

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

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

Solution

- World Writable Files:

- It is recommended that write access is removed from other with the command (`chmod o-w <filename>`), but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.

- World Writable Directories:

- Set the sticky bit on all world writable directories with the command (`chmod a+t <directory_name>`)

Run the following script to:

- Remove other write permission from any world writable files

- Add the sticky bit to all world writable directories

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

```
{ I_smask='01000'
```

```
a_file=(); a_dir=() # Initialize arrays a_path=( ! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path "*/containerd/*" -a ! -path "*/kubelet/pods/*" -a ! -path "*/kubelet/plugins/*" -a ! -path "/sys/*" -a ! -path "/snap/*") while IFS= read -r I_mount; do while IFS= read -r -d $'0' I_file; do if [ -e "$I_file" ]; then I_mode="$(stat -Lc '%#a' "$I_file")"
```

```
if [ -f "$I_file" ]; then # Remove excess permissions from WW files echo -e " - File: \"$I_file\" is mode: \"$I_mode\""
```

```
- removing write permission on \"$I_file\" from \"other\""
```

```
chmod o-w "$I_file"
```

```
fi if [ -d "$I_file" ]; then # Add sticky bit if [ ! $(( $I_mode & $I_smask )) -gt 0 ]; then echo -e " - Directory: \"$I_file\" is mode: \"$I_mode\" and doesn't have the sticky bit set"
```

```
- Adding the sticky bit"
```

```
chmod a+t "$I_file"
```



```
fi fi fi done <<(find "$l_mount" -xdev ( "${a_path[@]}" ) ( -type f -o -type d ) -perm -0002 -print0 2> /dev/null)
done <<(findmnt -Dkerno fstype,target | awk '($1 !~ /^s*(nfs|proc|smb|vfat|iso9660|efivarfs|selinuxfs)/
&& $2 !~ /^(run/user|/tmp|/var/tmp)/){print $2}') }
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10

CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2

PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

name: find_world_writeable_files

Hosts

192.168.40.171

The following 35 files are world writeable:

```

/var/www/rise.com/MF-Web-Backend/bootstrap/cache/.gitignore
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/bootstrap/app.php
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/public/robots.txt
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/public/index.php
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/public/favicon.ico
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/public/images/aliceologo.png
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/public/docs/openapi.yaml
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/public/docs/images/navbar.png
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/public/docs/collection.json
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/public/docs/index.html
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/public/.htaccess
  owner: mf_dev, group: mf_dev, permissions: 0777

```

```
/var/www/rise.com/MF-Web-Backend/storage/app/.gitignore
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/storage/logs/laravel.log
  owner: root, group: root, permissions: 0777

/var/www/rise.com/MF-Web-Backend/storage/logs/.gitignore
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/storage/framework/views/4b3946cd9b8aca740980736da9b76b00.php
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/storage/framework/views/6221e76a57dbfc41498adb0430b43891.php
  owner: mf_dev, group: mf_dev, permissions: 0777

/var/www/rise.com/MF-Web-Backend/storage/framework/views/f1fb36fb9e7eb8da6fc621cac1802b9d.php
  owner: mf_dev, group: mf_dev, permissio [...]
```

7.1.12 Ensure no files or directories without an owner and a group exist

Info

Administrators may delete users or groups from the system and neglect to remove all files and/or directories owned by those users or groups.

A new user or group who is assigned a deleted user's user ID or group ID may then end up "owning" a deleted user or group's files, and thus have more access on the system than was intended.

Solution

Remove or set ownership and group ownership of these files and/or directories to an active user on the system as appropriate.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)

CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s***\s]*pass:[\s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** FAIL **
- * Reasons for audit failure * :

  - There are "1" unowned files or directories on the system.
  - The following is a list of unowned files and/or directories:
/var/lib/docker/overlay2/2dda0827a6d7a80d3911fe4e201a8495f0049aed7b0f66d1e8055130a7b668da/diff/var/
cache/apt/archives/partial
  - end of list

- * Correctly configured * :

  - No files or directories without a group exist on the local filesystem.
```

Compliance 'SKIPPED'

Compliance 'PASSED'

1.1.1.1 Ensure cramfs kernel module is not available

Info

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

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

Solution

Run the following script to unload and disable the cramfs module:

- IF - the cramfs kernel module is available in ANY installed kernel:
- Create a file ending inconf with install cramfs /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with blacklist cramfs in the /etc/modprobe.d/ directory
- Run modprobe -r cramfs 2>/dev/null; rmmod cramfs 2>/dev/null to remove cramfs from the kernel
- IF - the cramfs kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

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

```
{ a_output2=() a_output3=() I_dl="" I_mod_name="cramfs" I_mod_type="fs"
I_mod_path="$(readlink -f /lib/modules/**/kernel/$I_mod_type | sort -u)"
f_module_fix() { I_dl="y" a_showconfig=() while IFS= read -r I_showconfig; do a_showconfig
+="$I_showconfig" done < <(modprobe --showconfig | grep -P -- 'b(install|blacklist)h
+""${I_mod_chk_name//-/}_"'b') if lsmod | grep "$I_mod_chk_name" &> /dev/null; then a_output2+=("
- unloading kernel module: \"$I_mod_name\"") modprobe -r "$I_mod_chk_name" 2>/dev/null; rmmod
"$I_mod_name" 2>/dev/null fi if ! grep -Pq -- 'binstallh+""${I_mod_chk_name//-/}_"'h+(/usr)?/bin/(true|
false)b' <<< "${a_showconfig[*]}"; then a_output2+=(" - setting kernel module: \"$I_mod_name\" to
\"$(readlink -f /bin/false)\"") printf '%s ' "install $I_mod_chk_name $(readlink -f /bin/false)" >> /etc/
modprobe.d/"$I_mod_name".conf fi if ! grep -Pq -- 'bblacklisth+""${I_mod_chk_name//-/}_"'b' <<<
"${a_showconfig[*]}"; then a_output2+=(" - denylisting kernel module: \"$I_mod_name\"") printf '%s '
"blacklist $I_mod_chk_name" >> /etc/modprobe.d/"$I_mod_name".conf fi } for I_mod_base_directory
in $I_mod_path; do # Check if the module exists on the system if [ -d "$I_mod_base_directory/
${I_mod_name//-/}_/" ] && [ -n "$(ls -A "$I_mod_base_directory/${I_mod_name//-/}_")" ]; then a_output3+=("
\"$I_mod_base_directory\"") I_mod_chk_name="$I_mod_name"
[[ "$I_mod_name" =~ overlay ]] && I_mod_chk_name="${I_mod_name::-2}"
[ "$I_dl" != "y" ] && f_module_fix else printf '%s ' " - kernel module: \"$I_mod_name\" doesn't exist in
\"$I_mod_base_directory\""
fi done [ "${#a_output3[@]}" -gt 0 ] && printf '%s ' "" -- INFO -- " - module: \"$I_mod_name\" exists in:"
"${a_output3[@]}"
[ "${#a_output2[@]}" -gt 0 ] && printf '%s ' "" "${a_output2[@]}" | | printf '%s ' "" - No changes needed"
printf '%s ' "" - remediation of kernel module: \"$I_mod_name\" complete" ""
}
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***[s]*pass:[s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
-- INFO --
- module: "cramfs" exists in:
```

```
- "/usr/lib/modules/6.8.0-60-generic/kernel/fs"
- "/usr/lib/modules/6.8.0-62-generic/kernel/fs"

- Audit Result:
  ** PASS **
  - kernel module: "cramfs" is not loaded
  - kernel module: "cramfs" is not loadable
  - kernel module: "cramfs" is deny listed
```

1.1.1.2 Ensure freevxfs kernel module is not available

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.

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

Solution

Run the following script to unload and disable the freevxfs module:

- IF - the freevxfs kernel module is available in ANY installed kernel:
- Create a file ending inconf with install freevxfs /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with blacklist freevxfs in the /etc/modprobe.d/ directory
- Run modprobe -r freevxfs 2>/dev/null; rmmod freevxfs 2>/dev/null to remove freevxfs from the kernel
- IF - the freevxfs kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

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

```
{ a_output2=() a_output3=() I_dl="" I_mod_name="freevxfs" I_mod_type="fs"
I_mod_path="$(readlink -f /lib/modules/**/kernel/$I_mod_type | sort -u)"
f_module_fix() { I_dl="y" a_showconfig=() while IFS= read -r I_showconfig; do a_showconfig
+="$I_showconfig" done < <(modprobe --showconfig | grep -P -- 'b(install|blacklist)h
+""${I_mod_chk_name//-/}_"'b') if lsmod | grep "$I_mod_chk_name" &> /dev/null; then a_output2+=("
- unloading kernel module: \"$I_mod_name\"") modprobe -r \"$I_mod_chk_name" 2>/dev/null; rmmod
"$I_mod_name" 2>/dev/null fi if ! grep -Pq -- 'binstallh+""${I_mod_chk_name//-/}_"'h+(/usr)?/bin/(true|
false)b' <<< "${a_showconfig[*]}"; then a_output2+=(" - setting kernel module: \"$I_mod_name\" to
\"$(readlink -f /bin/false)\"") printf '%s ' "install $I_mod_chk_name $(readlink -f /bin/false)" >> /etc/
modprobe.d/"$I_mod_name".conf fi if ! grep -Pq -- 'bblacklisth+""${I_mod_chk_name//-/}_"'b' <<<
"${a_showconfig[*]}"; then a_output2+=(" - denylisting kernel module: \"$I_mod_name\"") printf '%s '
"blacklist $I_mod_chk_name" >> /etc/modprobe.d/"$I_mod_name".conf fi } for I_mod_base_directory
in $I_mod_path; do # Check if the module exists on the system if [ -d "$I_mod_base_directory/
${I_mod_name//-/}_/" ] && [ -n "$(ls -A "$I_mod_base_directory/${I_mod_name//-/}_")" ]; then a_output3+=("
\"$I_mod_base_directory\"") I_mod_chk_name="$I_mod_name"
[[ "$I_mod_name" =~ overlay ]] && I_mod_chk_name="${I_mod_name::-2}"
[ "$I_dl" != "y" ] && f_module_fix else printf '%s ' " - kernel module: \"$I_mod_name\" doesn't exist in
\"$I_mod_base_directory\""
fi done [ "${#a_output3[@]}" -gt 0 ] && printf '%s ' "" -- INFO -- " - module: \"$I_mod_name\" exists in:"
"${a_output3[@]}"
[ "${#a_output2[@]}" -gt 0 ] && printf '%s ' "" "${a_output2[@]}" || printf '%s ' "" - No changes needed"
printf '%s ' "" - remediation of kernel module: \"$I_mod_name\" complete" ""
}
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***[s]*pass:[s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
-- INFO --
- module: "freevxfs" exists in:
```

```
- "/usr/lib/modules/6.8.0-60-generic/kernel/fs"
- "/usr/lib/modules/6.8.0-62-generic/kernel/fs"

- Audit Result:
  ** PASS **
  - kernel module: "freevxfs" is not loaded
  - kernel module: "freevxfs" is not loadable
  - kernel module: "freevxfs" is deny listed
```

1.1.1.3 Ensure hfs kernel module is not available

Info

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

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

Solution

Run the following script to unload and disable the hfs module:

- IF - the hfs kernel module is available in ANY installed kernel:
- Create a file ending inconf with install hfs /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with blacklist hfs in the /etc/modprobe.d/ directory
- Run modprobe -r hfs 2>/dev/null; rmmod hfs 2>/dev/null to remove hfs from the kernel
- IF - the hfs kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

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

```
{ a_output2=() a_output3=() I_dl="" I_mod_name="hfs" I_mod_type="fs"
I_mod_path="$(readlink -f /lib/modules/**/kernel/$I_mod_type | sort -u)"
f_module_fix() { I_dl="y" a_showconfig=() while IFS= read -r I_showconfig; do a_showconfig
+="$I_showconfig" done < <(modprobe --showconfig | grep -P -- 'b(install|blacklist)h
+""${I_mod_chk_name//-/}_""b') if lsmod | grep "$I_mod_chk_name" &> /dev/null; then a_output2+=("
- unloading kernel module: \"$I_mod_name\"") modprobe -r "$I_mod_chk_name" 2>/dev/null; rmmod
"$I_mod_name" 2>/dev/null fi if ! grep -Pq -- 'binstallh+""${I_mod_chk_name//-/}_""h+(/usr)?/bin/(true|
false)b' <<< "${a_showconfig[*]}"; then a_output2+=(" - setting kernel module: \"$I_mod_name\" to
\"$(readlink -f /bin/false)\"") printf '%s ' "install $I_mod_chk_name $(readlink -f /bin/false)" >> /etc/
modprobe.d/"$I_mod_name".conf fi if ! grep -Pq -- 'bblacklisth+""${I_mod_chk_name//-/}_""b' <<<
"${a_showconfig[*]}"; then a_output2+=(" - denylisting kernel module: \"$I_mod_name\"") printf '%s '
"blacklist $I_mod_chk_name" >> /etc/modprobe.d/"$I_mod_name".conf fi } for I_mod_base_directory
in $I_mod_path; do # Check if the module exists on the system if [ -d "$I_mod_base_directory/
${I_mod_name//-/}_/" ] && [ -n "$(ls -A "$I_mod_base_directory/${I_mod_name//-/}_")" ]; then a_output3+=(" -
\"$I_mod_base_directory\") I_mod_chk_name="$I_mod_name"
[[ "$I_mod_name" =~ overlay ]] && I_mod_chk_name="${I_mod_name::-2}"
[ "$I_dl" != "y" ] && f_module_fix else printf '%s ' " - kernel module: \"$I_mod_name\" doesn't exist in
\"$I_mod_base_directory\""
fi done [ "${#a_output3[@]}" -gt 0 ] && printf '%s ' "" -- INFO -- " - module: \"$I_mod_name\" exists in:"
"${a_output3[@]}"
[ "${#a_output2[@]}" -gt 0 ] && printf '%s ' "" "${a_output2[@]}" || printf '%s ' "" - No changes needed"
printf '%s ' "" - remediation of kernel module: \"$I_mod_name\" complete" ""
}
```

See Also

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?!)[\s]***[\s]*pass:[\s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
-- INFO --
- module: "hfs" exists in:
- "/usr/lib/modules/6.8.0-60-generic/kernel/fs"
- "/usr/lib/modules/6.8.0-62-generic/kernel/fs"
```

```
- Audit Result:  
  ** PASS **  
  - kernel module: "hfs" is not loaded  
  - kernel module: "hfs" is not loadable  
  - kernel module: "hfs" is deny listed
```

1.1.1.4 Ensure hfsplus kernel module is not available

Info

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

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

Solution

Run the following script to unload and disable the hfsplus module:

- IF - the hfsplus kernel module is available in ANY installed kernel:
- Create a file ending inconf with install hfsplus /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with blacklist hfsplus in the /etc/modprobe.d/ directory
- Run modprobe -r hfsplus 2>/dev/null; rmmod hfsplus 2>/dev/null to remove hfsplus from the kernel
- IF - the hfsplus kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

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

```
{ a_output2=() a_output3=() I_dl="" I_mod_name="hfsplus" I_mod_type="fs"
I_mod_path="$(readlink -f /lib/modules/**/kernel/$I_mod_type | sort -u)"
f_module_fix() { I_dl="y" a_showconfig=() while IFS= read -r I_showconfig; do a_showconfig
+="$I_showconfig" done < <(modprobe --showconfig | grep -P -- 'b(install|blacklist)h
+""${I_mod_chk_name//-/}_""b') if lsmod | grep "$I_mod_chk_name" &> /dev/null; then a_output2+=("
- unloading kernel module: \"$I_mod_name\"") modprobe -r "$I_mod_chk_name" 2>/dev/null; rmmod
"$I_mod_name" 2>/dev/null fi if ! grep -Pq -- 'binstallh+""${I_mod_chk_name//-/}_""h+(/usr)?/bin/(true|
false)b' <<< "${a_showconfig[*]}"; then a_output2+=(" - setting kernel module: \"$I_mod_name\" to
\"$(readlink -f /bin/false)\"") printf '%s ' "install $I_mod_chk_name $(readlink -f /bin/false)" >> /etc/
modprobe.d/"$I_mod_name".conf fi if ! grep -Pq -- 'bblacklisth+""${I_mod_chk_name//-/}_""b' <<<
"${a_showconfig[*]}"; then a_output2+=(" - denylisting kernel module: \"$I_mod_name\"") printf '%s '
"blacklist $I_mod_chk_name" >> /etc/modprobe.d/"$I_mod_name".conf fi } for I_mod_base_directory
in $I_mod_path; do # Check if the module exists on the system if [ -d "$I_mod_base_directory/
${I_mod_name//-/}_/" ] && [ -n "$(ls -A "$I_mod_base_directory/${I_mod_name//-/}_")" ]; then a_output3+=(" -
\"$I_mod_base_directory\"") I_mod_chk_name="$I_mod_name"
[[ "$I_mod_name" =~ overlay ]] && I_mod_chk_name="${I_mod_name::-2}"
[ "$I_dl" != "y" ] && f_module_fix else printf '%s ' " - kernel module: \"$I_mod_name\" doesn't exist in
\"$I_mod_base_directory\""
fi done [ "${#a_output3[@]}" -gt 0 ] && printf '%s ' "" -- INFO -- " - module: \"$I_mod_name\" exists in:"
"${a_output3[@]}"
[ "${#a_output2[@]}" -gt 0 ] && printf '%s ' "" "${a_output2[@]}" | printf '%s ' "" - No changes needed"
printf '%s ' "" - remediation of kernel module: \"$I_mod_name\" complete" ""
}
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***[s]*pass:[s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
-- INFO --  
- module: "hfsplus" exists in:
```

```
- "/usr/lib/modules/6.8.0-60-generic/kernel/fs"
- "/usr/lib/modules/6.8.0-62-generic/kernel/fs"

- Audit Result:
  ** PASS **
  - kernel module: "hfsplus" is not loaded
  - kernel module: "hfsplus" is not loadable
  - kernel module: "hfsplus" is deny listed
```

1.1.1.5 Ensure jffs2 kernel module is not available

Info

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

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

Solution

Run the following script to unload and disable the jffs2 module:

- IF - the jffs2 kernel module is available in ANY installed kernel:
- Create a file ending inconf with install jffs2 /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with blacklist jffs2 in the /etc/modprobe.d/ directory
- Run modprobe -r jffs2 2>/dev/null; rmmod jffs2 2>/dev/null to remove jffs2 from the kernel
- IF - the jffs2 kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

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

```
{ a_output2=() a_output3=() I_dl="" I_mod_name="jffs2" I_mod_type="fs"
I_mod_path="$(readlink -f /lib/modules/**/kernel/$I_mod_type | sort -u)"
f_module_fix() { I_dl="y" a_showconfig=() while IFS= read -r I_showconfig; do a_showconfig
+="$($I_showconfig)" done < <(modprobe --showconfig | grep -P -- 'b(install|blacklist)h
+""${I_mod_chk_name//-/}_"'b') if lsmod | grep "$I_mod_chk_name" &> /dev/null; then a_output2+=("
- unloading kernel module: \"$I_mod_name\"") modprobe -r "$I_mod_chk_name" 2>/dev/null; rmmod
"$I_mod_name" 2>/dev/null fi if ! grep -Pq -- 'binstallh+""${I_mod_chk_name//-/}_"'h+(/usr)?/bin/(true|
false)b' <<< "${a_showconfig[*]}"; then a_output2+=(" - setting kernel module: \"$I_mod_name\" to
\"$(readlink -f /bin/false)\"") printf '%s ' "install $I_mod_chk_name $(readlink -f /bin/false)" >> /etc/
modprobe.d/"$I_mod_name".conf fi if ! grep -Pq -- 'bblacklisth+""${I_mod_chk_name//-/}_"'b' <<<
"${a_showconfig[*]}"; then a_output2+=(" - denylisting kernel module: \"$I_mod_name\"") printf '%s '
"blacklist $I_mod_chk_name" >> /etc/modprobe.d/"$I_mod_name".conf fi } for I_mod_base_directory
in $I_mod_path; do # Check if the module exists on the system if [ -d "$I_mod_base_directory/
${I_mod_name//-/}_/" ] && [ -n "$(ls -A "$I_mod_base_directory/${I_mod_name//-/}_")" ]; then a_output3+=(" -
\"$I_mod_base_directory\"") I_mod_chk_name="$I_mod_name"
[[ "$I_mod_name" =~ overlay ]] && I_mod_chk_name="${I_mod_name::-2}"
[ "$I_dl" != "y" ] && f_module_fix else printf '%s ' " - kernel module: \"$I_mod_name\" doesn't exist in
\"$I_mod_base_directory\""
fi done [ "${#a_output3[@]}" -gt 0 ] && printf '%s ' "" -- INFO -- " - module: \"$I_mod_name\" exists in:"
"${a_output3[@]}"
[ "${#a_output2[@]}" -gt 0 ] && printf '%s ' "" "${a_output2[@]}" || printf '%s ' "" - No changes needed"
printf '%s ' "" - remediation of kernel module: \"$I_mod_name\" complete" ""
}
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***[s]*pass:[s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
-- INFO --  
- module: "jffs2" exists in:
```

```
- "/usr/lib/modules/6.8.0-60-generic/kernel/fs"
- "/usr/lib/modules/6.8.0-62-generic/kernel/fs"

- Audit Result:
  ** PASS **
- kernel module: "jffs2" is not loaded
- kernel module: "jffs2" is not loadable
- kernel module: "jffs2" is deny listed
```


1.1.1.9 Ensure usb-storage kernel module is not available

Info

USB storage provides a means to transfer and store files ensuring 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.

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

Solution

Run the following script to unload and disable the usb-storage module:

- IF - the usb-storage kernel module is available in ANY installed kernel:
- Create a file ending inconf with install usb-storage /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with blacklist usb-storage in the /etc/modprobe.d/ directory
- Run modprobe -r usb-storage 2>/dev/null; rmmod usb-storage 2>/dev/null to remove usb-storage from the kernel
- IF - the usb-storage kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

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

```
{ a_output2=() a_output3=() I_dl="" I_mod_name="usb-storage" I_mod_type="drivers"
I_mod_path="$(readlink -f /lib/modules/**/kernel/$I_mod_type | sort -u)"
f_module_fix() { I_dl="y" a_showconfig=() while IFS= read -r I_showconfig; do a_showconfig
+="$I_showconfig" done < <(modprobe --showconfig | grep -P -- 'b(install|blacklist)h
+""${I_mod_chk_name//-/}_}"b') if lsmod | grep "$I_mod_chk_name" &> /dev/null; then a_output2+=("
- unloading kernel module: \"$I_mod_name\"") modprobe -r \"$I_mod_chk_name" 2>/dev/null; rmmod
"$I_mod_name" 2>/dev/null fi if ! grep -Pq -- 'binstallh+""${I_mod_chk_name//-/}_}"h+(/usr)?/bin/(true|
false)b' <<< "${a_showconfig[*]}"; then a_output2+=(" - setting kernel module: \"$I_mod_name\" to
\"$(readlink -f /bin/false)\"") printf '%s ' "install $I_mod_chk_name $(readlink -f /bin/false)" >> /etc/
modprobe.d/"$I_mod_name".conf fi if ! grep -Pq -- 'bblacklisth+""${I_mod_chk_name//-/}_}"b' <<<
"${a_showconfig[*]}"; then a_output2+=(" - denylisting kernel module: \"$I_mod_name\"") printf '%s '
"blacklist $I_mod_chk_name" >> /etc/modprobe.d/"$I_mod_name".conf fi } for I_mod_base_directory
in $I_mod_path; do # Check if the module exists on the system if [ -d "$I_mod_base_directory/
${I_mod_name//-/}_}" ] && [ -n "$(ls -A "$I_mod_base_directory/${I_mod_name//-/}_}")" ]; then a_output3+=(" -
\"$I_mod_base_directory\") I_mod_chk_name="$I_mod_name"
[[ "$I_mod_name" =~ overlay ]] && I_mod_chk_name="${I_mod_name::-2}"
[ "$I_dl" != "y" ] && f_module_fix else printf '%s ' " - kernel module: \"$I_mod_name\" doesn't exist in
\"$I_mod_base_directory\""
fi done [ "${#a_output3[@]}" -gt 0 ] && printf '%s ' "" -- INFO -- " - module: \"$I_mod_name\" exists in:"
"${a_output3[@]}"
[ "${#a_output2[@]}" -gt 0 ] && printf '%s ' "" "${a_output2[@]}" | printf '%s ' "" - No changes needed"
printf '%s ' "" - remediation of kernel module: \"$I_mod_name\" complete" ""
```

}

Impact:

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.8.7
800-171R3	03.08.07
800-53	MP-7
800-53R5	MP-7
CN-L3	8.5.4.1(c)
CSCV7	13.7
CSCV8	10.3
CSF	PR.PT-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.7.10
ISO/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
NESA	T1.4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?!)[\s]***[\s]*pass:[\s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
-- INFO --  
- module: "usb-storage" exists in:
```

```
- "/usr/lib/modules/6.8.0-60-generic/kernel/drivers"
- "/usr/lib/modules/6.8.0-62-generic/kernel/drivers"

- Audit Result:
  ** PASS **
  - kernel module: "usb-storage" is not loaded
  - kernel module: "usb-storage" is not loadable
  - kernel module: "usb-storage" is deny listed
```

1.1.2.1.1 Ensure /tmp is a separate partition

Info

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

- IF - an entry for /tmp exists in /etc/fstab it will take precedence over entries in systemd default unit file.

Note: In an environment where the main system is diskless and connected to iSCSI, entries in /etc/fstab may not take precedence.

/tmp can be configured to use tmpfs

tmpfs puts everything into the kernel internal caches and grows and shrinks to accommodate the files it contains and is able to swap unneeded pages out to swap space. It has maximum size limits which can be adjusted on the fly via mount -o remount

Since tmpfs lives completely in the page cache and on swap, all tmpfs pages will be shown as "Shmem" in /proc/meminfo and "Shared" in free. Notice that these counters also include shared memory. The most reliable way to get the count is using df and du

tmpfs has three mount options for sizing:

- size : The limit of allocated bytes for this tmpfs instance. The default is half of your physical RAM without swap. If you oversize your tmpfs instances the machine will deadlock since the OOM handler will not be able to free that memory.
- nr_blocks : The same as size, but in blocks of PAGE_SIZE.
- nr_inodes : The maximum number of inodes for this instance. The default is half of the number of your physical RAM pages, or (on a machine with highmem) the number of lowmem RAM pages, whichever is the lower.

These parameters accept a suffix k, m or g and can be changed on remount. The size parameter also accepts a suffix % to limit this tmpfs instance to that percentage of your physical RAM. The default, when neither size nor nr_blocks is specified, is size=50%

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

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

Solution

First ensure that systemd is correctly configured to ensure that /tmp will be mounted at boot time.

```
# systemctl unmask tmp.mount
```

For specific configuration requirements of the /tmp mount for your environment, modify /etc/fstab

Example of using tmpfs with specific mount options:

tmpfs/tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime,size=2G 0 0

Note: the size=2G is an example of setting a specific size for tmpfs

Example of using a volume or disk with specific mount options. The source location of the volume or disk will vary depending on your environment:

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

Impact:

By design files saved to /tmp should have no expectation of surviving a reboot of the system. tmpfs is ram based and all files stored to tmpfs will be lost when the system is rebooted.

If files need to be persistent through a reboot, they should be saved to /var/tmp not /tmp

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9

ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/findmnt -nk /tmp expect: ^[\s]*/tmp[\s]+

Hosts

192.168.40.171

```
The command '/bin/findmnt -nk /tmp' returned :
```

```
/tmp    tmpfs    tmpfs    rw,nosuid,nodev,noexec,relatime,size=4194304k,inode64
```

1.1.2.1.2 Ensure nodev option set on /tmp partition

Info

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

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

Solution

- IF - a separate partition exists for /tmp

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

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6

ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/tmp[\s]+ required: NO

Hosts

192.168.40.171

```
Compliant file(s):
  /proc/self/mountinfo - regex '[\s]+/tmp[\s]+' found - expect 'nodev' found in the following
  lines:
    27: 60 29 0:34 / /tmp rw,nosuid,nodev,noexec,relatime shared:58 - tmpfs tmpfs
    rw,size=4194304k,inode64
```


1.1.2.1.3 Ensure nosuid option set on /tmp partition

Info

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

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

- IF - a separate partition exists for /tmp

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

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/tmp[\s]+ required: NO

Hosts

192.168.40.171

```
Compliant file(s):
    /proc/self/mountinfo - regex '[\s]+/tmp[\s]+' found - expect 'nosuid' found in the following
lines:
    27: 60 29 0:34 / /tmp rw,nosuid,nodev,noexec,relatime shared:58 - tmpfs tmpfs
    rw,size=4194304k,inode64
```

1.1.2.1.4 Ensure noexec option set on /tmp partition

Info

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

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

- IF - a separate partition exists for /tmp

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

Example:

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

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

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

Impact:

Setting the noexec option on /tmp may prevent installation and/or updating of some 3rd party software.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5

800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2

NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: noexec file: /proc/self/mountinfo regex: [\s]+/tmp[\s]+ required: NO

Hosts

192.168.40.171

```
Compliant file(s):
    /proc/self/mountinfo - regex '[\s]+/tmp[\s]+' found - expect 'noexec' found in the following
    lines:
```

```
27: 60 29 0:34 / /tmp rw,nosuid,nodev,noexec,relatime shared:58 - tmpfs tmpfs
rw,size=4194304k,inode64
```

1.1.2.2.1 Ensure /dev/shm is a separate partition

Info

The /dev/shm directory is a world-writable directory that can function as shared memory that facilitates inter process communication (IPC).

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

This can be accomplished by mounting tmpfs to /dev/shm

Solution

For specific configuration requirements of the /dev/shm mount for your environment, modify /etc/fstab

Example:

```
tmpfs/dev/shmtmpfs defaults,rw,nosuid,nodev,noexec,relatime,size=2G 0 0
```

Impact:

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

/dev/shm utilizing tmpfs can be resized using the size={size} parameter in the relevant entry in /etc/fstab

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1

CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: [\s]+/dev/shm[\s]+ file: /proc/self/mountinfo regex: [\s]+/dev/shm[\s]+ required: NO

Hosts

192.168.40.171

```
Compliant file(s):
  /proc/self/mountinfo - regex '[\s]+/dev/shm[\s]+' found - expect '[\s]+/dev/shm[\s]+' found in
  the following lines:
    8: 31 26 0:26 / /dev/shm rw,nosuid,nodev,noexec,relatime shared:4 - tmpfs tmpfs rw,inode64
```

1.1.2.2.2 Ensure nodev option set on /dev/shm partition

Info

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

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

- IF - a separate partition exists for /dev/shm

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

Example:

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

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5

800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2

NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/dev/shm[\s]+ required: NO

Hosts

192.168.40.171

```
Compliant file(s):
    /proc/self/mountinfo - regex '[\s]+/dev/shm[\s]+' found - expect 'nodev' found in the
    following lines:
```

```
8: 31 26 0:26 / /dev/shm rw,nosuid,nodev,noexec,relatime shared:4 - tmpfs tmpfs rw,inode64
```

1.1.2.2.3 Ensure nosuid option set on /dev/shm partition

Info

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

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

- IF - a separate partition exists for /dev/shm

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

Example:

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

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5

800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2

NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/dev/shm[\s]+ required: NO

Hosts

192.168.40.171

```
Compliant file(s):
    /proc/self/mountinfo - regex '[\s]+/dev/shm[\s]+' found - expect 'nosuid' found in the
    following lines:
```



```
8: 31 26 0:26 / /dev/shm rw,nosuid,nodev,noexec,relatime shared:4 - tmpfs tmpfs rw,inode64
```

1.1.2.2.4 Ensure noexec option set on /dev/shm partition

Info

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

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

- IF - a separate partition exists for /dev/shm

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

Example:

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

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5

800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2

NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: noexec file: /proc/self/mountinfo regex: [\s]+/dev/shm[\s]+ required: NO

Hosts

192.168.40.171

```
Compliant file(s):
    /proc/self/mountinfo - regex '[\s]+/dev/shm[\s]+' found - expect 'noexec' found in the
    following lines:
```

```
8: 31 26 0:26 / /dev/shm rw,nosuid,nodev,noexec,relatime shared:4 - tmpfs tmpfs rw,inode64
```

1.1.2.3.2 Ensure nodev option set on /home partition

Info

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

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

Solution

- IF - a separate partition exists for /home

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

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/home[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

1.1.2.3.3 Ensure nosuid option set on /home partition

Info

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

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

Solution

- IF - a separate partition exists for /home

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

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/home[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

1.1.2.4.2 Ensure nodev option set on /var partition

Info

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

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

Solution

- IF - a separate partition exists for /var

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

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/var[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

1.1.2.4.3 Ensure nosuid option set on /var partition

Info

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

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

Solution

- IF - a separate partition exists for /var

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

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/var[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

1.1.2.5.2 Ensure nodev option set on /var/tmp partition

Info

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

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

Solution

- IF - a separate partition exists for /var/tmp

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

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/var/tmp[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

1.1.2.5.3 Ensure nosuid option set on /var/tmp partition

Info

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

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

- IF - a separate partition exists for /var/tmp

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

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/var/tmp[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

1.1.2.5.4 Ensure noexec option set on /var/tmp partition

Info

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

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

- IF - a separate partition exists for /var/tmp

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

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: noexec file: /proc/self/mountinfo regex: [\s]+/var/tmp[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

1.1.2.6.2 Ensure nodev option set on /var/log partition

Info

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

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

Solution

- IF - a separate partition exists for /var/log

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

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/var/log[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

1.1.2.6.3 Ensure nosuid option set on /var/log partition

Info

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

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

Solution

- IF - a separate partition exists for /var/log

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

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/var/log[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

1.1.2.6.4 Ensure noexec option set on /var/log partition

Info

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

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

Solution

- IF - a separate partition exists for /var/log

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

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: noexec file: /proc/self/mountinfo regex: [\s]+/var/log[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

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

Info

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

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

Solution

- IF - a separate partition exists for /var/log/audit

Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /var/log/audit partition.

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/var/log/audit[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

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

Info

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

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

Solution

- IF - a separate partition exists for /var/log/audit

Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /var/log/audit partition.

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/var/log/audit[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

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

Info

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

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

Solution

- IF - a separate partition exists for /var/log/audit

Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /var/log/audit partition.

Example:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: noexec file: /proc/self/mountinfo regex: [\s]+/var/log/audit[\s]+ required: NO

Hosts

192.168.40.171

No matching files were found

1.2.2.1 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.

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.

Solution

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

```
# apt update
# apt upgrade
- OR - # apt dist-upgrade
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.11.2
800-171	3.11.3
800-171	3.14.1
800-171R3	03.11.02
800-171R3	03.14.01
800-53	RA-5
800-53	SI-2
800-53	SI-2(2)
800-53R5	RA-5
800-53R5	RA-7
800-53R5	SI-2
800-53R5	SI-2(2)
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
CSCV8	7.3
CSCV8	7.4
CSF	DE.CM-8
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.IP-12
CSF	RS.CO-3
CSF	RS.MI-3
CSF2.0	GV.SC-10
CSF2.0	ID.IM-01
CSF2.0	ID.IM-02
CSF2.0	ID.IM-03
CSF2.0	ID.RA-01
CSF2.0	ID.RA-08
CSF2.0	PR.PS-02
GDPR	32.1.b
GDPR	32.1.d
HIPAA	164.306(a)(1)
ISO-27001-2022	A.6.8
ISO-27001-2022	A.8.8
ISO-27001-2022	A.8.32
ISO/IEC-27001	A.12.6.1
ITSG-33	RA-5
ITSG-33	SI-2
ITSG-33	SI-2(2)
LEVEL	1M
NESA	M1.2.2
NESA	M5.4.1
NESA	T7.6.2
NESA	T7.7.1
NIAV2	PR9
PCI-DSSV3.2.1	6.1
PCI-DSSV3.2.1	6.2
PCI-DSSV4.0	6.3
PCI-DSSV4.0	6.3.1
PCI-DSSV4.0	6.3.3
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3

QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
SWIFT-CSCV1	2.2
SWIFT-CSCV1	2.7

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/apt-get -s upgrade | /bin/grep -Ev '(Reading|Building|Calculating)'
expect: ^[\s]*0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded

Hosts

192.168.40.171

```
The command '/bin/apt-get -s upgrade | /bin/grep -Ev '(Reading|Building|Calculating)'' returned :  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

1.3.1.1 Ensure AppArmor is installed

Info

AppArmor provides Mandatory Access Controls.

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

Solution

Install AppArmor.

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)

CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - dpkg check apparmor-utils

The command '/bin/dpkg -s apparmor-utils 2>&1 | /bin/grep -E '(Status:|not installed)'' returned :

Status: install ok installed

PASSED - dpkg check apparmor

The command '/bin/dpkg -s apparmor 2>&1 | /bin/grep -E '(Status:|not installed)'' returned :

Status: install ok installed

1.3.1.2 Ensure AppArmor is enabled in the bootloader configuration

Info

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

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

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 apparmor=1 and security=apparmor parameters to the GRUB_CMDLINE_LINUX= line

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

Run the following command to update the grub2 configuration:

```
# update-grub
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2

CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1

NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

```
-----
PASSED - grub.cfg security=apparmor
Compliant file(s):
    /boot/grub/grub.cfg - regex '^[s]*linux[s]*' found - expect '(?i)security=apparmor(?-i)'
    found in the following lines:
```

```

170: linux/vmlinuz-6.8.0-62-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro apparmor=1
security=apparmor ipv6.disable=1
189: linux/vmlinuz-6.8.0-62-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro apparmor=1
security=apparmor ipv6.disable=1
207: linux/vmlinuz-6.8.0-62-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro recovery
nomodeset dis_ucode_ldr apparmor=1 security=apparmor
226: linux/vmlinuz-6.8.0-60-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro apparmor=1
security=apparmor ipv6.disable=1
244: linux/vmlinuz-6.8.0-60-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro recovery
nomodeset dis_ucode_ldr apparmor=1 security=apparmor

-----
PASSED - grub.cfg apparmor=1
Compliant file(s):
    /boot/grub/grub.cfg - regex '^[s]*linux[s]*' found - expect '(?i)apparmor=1(?-i)' found in
the following lines:
    170: linux/vmlinuz-6.8.0-62-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro apparmor=1
security=apparmor ipv6.disable=1
    189: linux/vmlinuz-6.8.0-62-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro apparmor=1
security=apparmor ipv6.disable=1
    207: linux/vmlinuz-6.8.0-62-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro recovery
nomodeset dis_ucode_ldr apparmor=1 security=apparmor
    226: linux/vmlinuz-6.8.0-60-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro apparmor=1
security=apparmor ipv6.disable=1
    244: linux/vmlinuz-6.8.0-60-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro recovery
nomodeset dis_ucode_ldr apparmor=1 security=apparmor

```

1.3.1.3 Ensure all AppArmor Profiles are in enforce or complain mode

Info

AppArmor profiles define what resources applications are able to access.

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/*
```

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6

800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3

NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

```
-----
PASSED - apparmor_status - processes are confined
The command '/sbin/apparmor_status' returned :
```

```

apparmor module is loaded.
149 profiles are loaded.
54 profiles are in enforce mode.
/snap/snapd/23771/usr/lib/snapd/snap-confine
/snap/snapd/23771/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
/snap/snapd/24505/usr/lib/snapd/snap-confine
/snap/snapd/24505/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
/snap/snapd/24718/usr/lib/snapd/snap-confine
/snap/snapd/24718/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
/usr/bin/man
/usr/lib/snapd/snap-confine
/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
/usr/sbin/mysqld
docker-default
lsb_release
man_filter
man_groff
nvidia_modprobe
nvidia_modprobe//kmod
plasmashell
plasmashell//QtWebEngineProcess
rsyslogd
snap-update-ns.canonical-livepatch
snap-update-ns.lxd
snap.canonical-livepatch.canonical-livepatch
snap.canonical-livepatch.canonical-livepatchd
snap.canonical-livepatch.hook.configure
snap.canonical-livepatch.hook.connect-plug-etc-update-motd-d
snap.canonical-livepatch.hook.disconnect-plug-etc-update-motd-d
snap.canonical-livepatch.hook.post-refresh
snap.canonical-livepatch.hook.remove
snap.lxd.activate
snap.lxd.benchmark
snap.lxd.buginfo
snap.lxd.check-kernel
snap.lxd.daemon
snap.lxd.hook.configure
snap.lxd.hook.install
snap.lxd.hook.remove
snap.lxd.lxc
snap.lxd.lxc-to-lxd
snap.lxd.lxd
snap.lxd.migrate
snap.lxd.user-daemon
tcpdump
ubuntu_pro_apt_news
ubuntu_pro_esm_cache
ubuntu_pro_esm_cache//apt_methods
ubuntu_pro_esm_cache//apt_methods_gpgv
ubuntu_pro_esm_cache//cloud_id
ubuntu_pro_esm_cache//dpkg
ubuntu_pro_esm_cache//ps
ubuntu_pro_esm_cache//ubuntu_distro_info
ubuntu_pro_esm_cache_systemctl
ubuntu_pro_esm_cache_systemd_detect_virt
unix-chkpwd
unprivileged_usersns
4 profiles [...]

```

1.4.1 Ensure bootloader password is set

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

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 --iteration-count=600000 --salt=64
```

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 exec tail -n +2 $0 set superusers="<username>"
```

```
password_pbkdf2 <username> <encrypted-password>
```

```
EOF
```

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

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

Example:

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

Run the following command to update the grub2 configuration:

```
# update-grub
```

Impact:

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

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

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

More Information:

<https://help.ubuntu.com/community/Grub2/Passwords>

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10

CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2

PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - set superusers

Compliant file(s):

/boot/grub/grub.cfg - regex '^[\\s]*set[\\s]*superusers[\\s]*=' found - expect
 '^[\\s]*set[\\s]*superusers[\\s]*=\\.\\.\\.\\\$' found in the following lines:
 288: set superusers="root"

PASSED - password_pbkdf2

Compliant file(s):

/boot/grub/grub.cfg - regex '^[\\s]*password' found - expect '^[\\s]*password_pbkdf2[\\s]+[\\s]+[\\s]+[\\s]+[\\s]*\$' found in the following lines:
 289: password_pbkdf2 root

grub.pbkdf2.sha512.600000.0D4900694D15FC420C1D7B469CF760D2314B0CEF8B149F09A71B059F1132B331E202DA371AA754449CA4374

1.4.2 Ensure access to bootloader config is configured

Info

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)

CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /boot/grub/grub.cfg group: root mask: 7177 owner: root

Hosts

192.168.40.171

```
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
```

1.5.1 Ensure address space layout randomization 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.

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 file in `/etc/sysctl.d/` ending in `conf` :

- `kernel.randomize_va_space = 2`

Example:

```
# printf "%s " "kernel.randomize_va_space = 2" >> /etc/sysctl.d/60-kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-53	SI-16
800-53R5	SI-16
CSCV7	8.3
CSCV8	10.5
CSF2.0	PR.DS-10
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
LEVEL	1A

Audit File

`CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit`

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***\[s]*pass:[?]\[s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- "kernel.randomize_va_space" is correctly set to "2"
  in the running configuration
- "kernel.randomize_va_space" is correctly set to "2"
  in "/etc/sysctl.conf"
```

1.5.2 Ensure ptrace_scope is restricted

Info

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

The `sysctl` settings (writable only with `CAP_SYS_PTRACE`) are:

- 0 - classic ptrace permissions: a process can `PTRACE_ATTACH` to any other process running under the same uid, as long as it is dumpable (i.e. did not transition uids, start privileged, or have called `prctl(PR_SET_DUMPABLE...)` already). Similarly, `PTRACE_TRACEME` is unchanged.
- 1 - restricted ptrace: a process must have a predefined relationship with the inferior it wants to call `PTRACE_ATTACH` on. By default, this relationship is that of only its descendants when the above classic criteria is also met. To change the relationship, an inferior can call `prctl(PR_SET_PTRACER, debugger, ...)` to declare an allowed debugger PID to call `PTRACE_ATTACH` on the inferior. Using `PTRACE_TRACEME` is unchanged.
- 2 - admin-only attach: only processes with `CAP_SYS_PTRACE` may use ptrace with `PTRACE_ATTACH`, or through children calling `PTRACE_TRACEME`.
- 3 - no attach: no processes may use ptrace with `PTRACE_ATTACH` nor via `PTRACE_TRACEME`. Once set, this `sysctl` value cannot be changed.

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

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

Solution

Set the `kernel.yama.ptrace_scope` parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `conf` to a value of 1 2 or 3 :

```
kernel.yama.ptrace_scope = 1
```

```
- OR - kernel.yama.ptrace_scope = 2
```

```
- OR - kernel.yama.ptrace_scope = 3
```

Example:

```
# printf "%s " "kernel.yama.ptrace_scope = 1" >> /etc/sysctl.d/60-kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

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

Note:

- If a value of 2 or 3 is preferred, or required by local site policy, replace the 1 with the desired value of 2 or 3 in the example above
- If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]**\[s]*pass:[s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

- Audit Result:
** PASS **

- "kernel.yama.ptrace_scope" is correctly set to "1" in the running configuration
- "kernel.yama.ptrace_scope" is correctly set to "1" in "/etc/sysctl.d/10-ptrace.conf"

1.5.3 Ensure core dumps are restricted

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.

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 file in `/etc/sysctl.d/` ending in `conf`:

```
- fs.suid_dumpable = 0
```

Example:

```
# printf "%s" "fs.suid_dumpable = 0" >> /etc/sysctl.d/60-fs_sysctl.conf
```

Run the following command to set the active kernel parameter:

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

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

-If- `systemd-coredump` is installed:

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

```
Storage=none ProcessSizeMax=0
```

Run the command:

```
systemctl daemon-reload
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)

800-53R5	AC-6(10)
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
LEVEL	1A
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - hard core 0

Compliant file(s):

/etc/security/limits.conf - regex '^h*\\h+hard\\h+core\\h+0\\b' found - expect '^h*\\h+hard\\h+core\\h+0\\b' found in the following lines:
69: * hard core 0

PASSED - fs.suid_dumpable

The command script with multiple lines returned :

- Audit Result:

** PASS **

- "fs.suid_dumpable" is correctly set to "0"
in the running configuration
- "fs.suid_dumpable" is correctly set to "0"
in "/etc/sysctl.conf"

PASSED - check if systemd-coredump is installed

The command '/bin/systemctl list-unit-files | /bin/grep coredump | /bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

systemd-coredump@.service	static	-
systemd-coredump.socket	static	-
pass		

1.5.4 Ensure prelink is not installed

Info

prelink is a program that modifies ELF shared libraries and ELF dynamically linked binaries in such a way that the time needed for the dynamic linker to perform relocations at startup significantly decreases.

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/benchmarks/18959>

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.01
800-171R3	03.03.03
800-53	AC-6(9)
800-53	AU-2
800-53	AU-12
800-53R5	AC-6(9)
800-53R5	AU-2
800-53R5	AU-12
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSCV7	14.9
CSCV8	3.14
CSF	DE.CM-1

CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-2
ITSG-33	AU-12
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1

PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s prelink 2>&1 | /bin/grep -E '^(Status:|not installed)'

expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s prelink 2>&1 | /bin/grep -E '^(Status:|not installed)'' returned :
dpkg-query: package 'prelink' is not installed and no information is available
```

1.5.5 Ensure Automatic Error Reporting is not enabled

Info

The Apport Error Reporting Service automatically generates crash reports for debugging

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

Solution

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

```
enabled=0
```

Run the following commands to stop and mask the apport service

```
# systemctl stop apport.service # systemctl mask apport.service
```

- OR -

Run the following command to remove the apport package:

```
# apt purge apport
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)

ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

1.6.1 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

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/benchmarks/18959>

References

800-171	3.1.9
800-171R3	03.01.09
800-53	AC-8a.
800-53R5	AC-8a.
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-8a.
LEVEL	1A
NESA	M5.2.5
NESA	T5.5.1
NIIV2	AM10a

NIAV2	AM10b
NIAV2	AM10c
NIAV2	AM10d
NIAV2	AM10e
TBA-FIISB	45.2.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

1.6.4 Ensure access to /etc/motd is 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.

- IF - the /etc/motd file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

Solution

Run the following commands to set mode, owner, and group on /etc/motd :

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

- OR -

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/motd group: root mask: 133 owner: root required: NO

Hosts

192.168.40.171

1.6.5 Ensure access to /etc/issue is configured

Info

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

- IF - the /etc/issue file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

Solution

Run the following commands to set mode, owner, and group on /etc/issue :

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)

CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/issue group: root mask: 133 owner: root

Hosts

192.168.40.171

```
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
```

1.6.6 Ensure access to /etc/issue.net is configured

Info

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

- IF - the /etc/issue.net file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

Solution

Run the following commands to set mode, owner, and group on /etc/issue.net :

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)

CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/issue.net group: root mask: 133 owner: root

Hosts

192.168.40.171

```
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
```

1.7.2 Ensure GDM login banner is configured

Info

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

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

- IF - A user profile is already created run the following commands to set and enable the text banner message on the login screen:

```
# gsettings set org.gnome.login-screen banner-message-text 'Authorized users only. All activity may be monitored and reported' # gsettings set org.gnome.login-screen banner-message-enable true
```

Note:

- banner-message-text may be set in accordance with local site policy
- gsettings commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.
- The system must be restarted after all gsettings configurations have been set in order for CIS-CAT Assessor to appropriately assess.
- OR/IF - A user profile does not exist:
- Create or edit the gdm profile in the /etc/dconf/profile/gdm with the following lines:

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

Note: gdm is the name of a dconf database.

<xhtml:ol start="2"> - Create a gdm keyfile for machine-wide settings in /etc/dconf/db/gdm.d/01-banner-message :

```
[org/gnome/login-screen] banner-message-enable=true banner-message-text='Type the banner message here.'
```

<xhtml:ol start="3"> - Update the system databases

```
# dconf update
```

Note:

- Users must log out and back in again before the system-wide settings take effect.
- There is no character limit for the banner message. gnome-shell autodetects longer stretches of text and enters two column mode.
- The banner message cannot be read from an external file.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.9
800-171R3	03.01.09
800-53	AC-8
800-53R5	AC-8
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-8
LEVEL	1A
NESA	M1.3.6
TBA-FIISB	45.2.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

1.7.3 Ensure GDM disable-user-list option is enabled

Info

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

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

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

Solution

- IF - A user profile exists run the following command to enable the disable-user-list :

```
# gsettings set org.gnome.login-screen disable-user-list true
```

Note:

- gsettings commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.

- The system must be restarted after all gsettings configurations have been set in order for CIS-CAT Assessor to appropriately assess.

- OR/IF - A user profile does not exist:

- Create or edit the gdm profile in /etc/dconf/profile/gdm with the following lines:

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

Note: gdm is the name of a dconf database.

<xhtml:ol start="2"> - Create a gdm keyfile for machine-wide settings in /etc/dconf/db/gdm.d/00-login-screen :

[org/gnome/login-screen] # Do not show the user list disable-user-list=true <xhtml:ol start="3"> - Update the system databases:

```
# dconf update
```

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.11
800-171R3	03.05.11
800-53	IA-6
800-53R5	IA-6

CSF2.0	PR.AA-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
ISO-27001-2022	A.8.5
ITSG-33	IA-6
ITSG-33	IA-6a.
LEVEL	1A
NESA	T5.5.1
QCSC-V1	13.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

1.7.4 Ensure GDM screen locks when the user is idle

Info

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

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

Solution

- IF - A user profile is already created run the following commands to enable screen locks when the user is idle:

```
# gsettings set org.gnome.desktop.screensaver lock-delay 5 # gsettings set org.gnome.desktop.session idle-delay 900
```

Note:

- gsettings commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.

- The system must be restarted after all gsettings configurations have been set in order for CIS-CAT Assessor to appropriately assess.

- OR/IF- A user profile does not exist:

- Create or edit the user profile in the /etc/dconf/profile/ and verify it includes the following:

```
user-db:user system-db:{NAME_OF_DCONF_DATABASE}
```

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

<xhtml:ol start="2"> -

Create the directory /etc/dconf/db/local.d/ if it doesn't already exist:

-

Create the key file /etc/dconf/db/local.d/00-screensaver to provide information for the local database:

Example key file:

```
# Specify the dconf path [org/gnome/desktop/session]
```

```
# Number of seconds of inactivity before the screen goes blank # Set to 0 seconds if you want to deactivate the screensaver.
```

```
idle-delay=uint32 180
```

```
# Specify the dconf path [org/gnome/desktop/screensaver]
```

```
# Number of seconds after the screen is blank before locking the screen lock-delay=uint32 0
```

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

<xhtml:ol start="4"> - Run the following command to update the system databases:

dconf update <xhtml:ol start="5"> - Users must log out and back in again before the system-wide settings take effect.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.10
800-171	3.1.11
800-171R3	03.01.01h.
800-171R3	03.01.10
800-171R3	03.01.11
800-53	AC-2(5)
800-53	AC-11
800-53	AC-11(1)
800-53	AC-12
800-53R5	AC-2(5)
800-53R5	AC-11
800-53R5	AC-11(1)
800-53R5	AC-12
CN-L3	7.1.2.2(d)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.7(b)
CN-L3	8.1.4.1(b)
CSCV7	16.11
CSCV8	4.3
CSF	PR.AC-1
CSF	PR.AC-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18
ISO-27001-2022	A.7.7

ISO-27001-2022	A.8.1
ISO-27001-2022	A.8.2
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2(5)
ITSG-33	AC-11
ITSG-33	AC-11(1)
ITSG-33	AC-12
LEVEL	1A
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	NS5j
NIAV2	NS49
NIAV2	SS14e
PCI-DSSV3.2.1	8.1.8
PCI-DSSV4.0	8.2.8
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
TBA-FIISB	36.2.1
TBA-FIISB	37.1.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

1.7.5 Ensure GDM screen locks cannot be overridden

Info

GNOME Desktop Manager can lock down specific settings by using the lockdown mode in dconf to prevent users from changing specific settings.

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

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

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

Solution

- To prevent the user from overriding these settings, create the file `/etc/dconf/db/local.d/locks/00-screensaver` with the following content:

```
# Lock desktop screensaver settings /org/gnome/desktop/session/idle-delay /org/gnome/desktop/screensaver/lock-delay <xhtml:ol start="2"> - Update the system databases:
```

```
# dconf update
```

Note:

- A user profile must exist in order to apply locks.
- Users must log out and back in again before the system-wide settings take effect.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.10
800-171	3.1.11
800-171R3	03.01.01h.
800-171R3	03.01.10
800-171R3	03.01.11
800-53	AC-2(5)
800-53	AC-11
800-53	AC-11(1)
800-53	AC-12
800-53R5	AC-2(5)
800-53R5	AC-11

800-53R5	AC-11(1)
800-53R5	AC-12
CN-L3	7.1.2.2(d)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.7(b)
CN-L3	8.1.4.1(b)
CSCV7	16.11
CSCV8	4.3
CSF	PR.AC-1
CSF	PR.AC-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18
ISO-27001-2022	A.7.7
ISO-27001-2022	A.8.1
ISO-27001-2022	A.8.2
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2(5)
ITSG-33	AC-11
ITSG-33	AC-11(1)
ITSG-33	AC-12
LEVEL	1A
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	NS5j
NIAV2	NS49
NIAV2	SS14e
PCI-DSSV3.2.1	8.1.8
PCI-DSSV4.0	8.2.8
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2

QCSC-V1	15.2
TBA-FIISB	36.2.1
TBA-FIISB	37.1.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

1.7.6 Ensure GDM automatic mounting of removable media is disabled

Info

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

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

- IF - A user profile exists run the following commands to ensure automatic mounting is disabled:

```
# gsettings set org.gnome.desktop.media-handling automount false # gsettings set  
org.gnome.desktop.media-handling automount-open false
```

Note:

- gsettings commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.

- The system must be restarted after all gsettings configurations have been set in order for CIS-CAT Assessor to appropriately assess.

- OR/IF - A user profile does not exist:

- Create a file /etc/dconf/db/local.d/00-media-automount with following content:

[org/gnome/desktop/media-handling] automount=false automount-open=false <html:ol start="2"> - After creating the file, apply the changes using below command :

```
# dconf update
```

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

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.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.8.7
800-171R3	03.08.07
800-53	MP-7
800-53R5	MP-7
CN-L3	8.5.4.1(c)
CSCV7	8.5

CSCV8	10.3
CSF	PR.PT-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.7.10
ISO/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
NESA	T1.4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

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

Info

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

By using the lockdown mode in dconf, you can prevent users from changing specific settings. To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.

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

- To prevent the user from overriding these settings, create the file `/etc/dconf/db/local.d/locks/00-media-automount` with the following content:

`[org/gnome/desktop/media-handling] automount=false automount-open=false` <html:ol start="2"> -
Update the systems databases:

`# dconf update`

Note:

- A user profile must exist in order to apply locks.
- Users must log out and back in again before the system-wide settings take effect.

Impact:

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.08.02
800-53	MP-2
800-53R5	MP-2
CSF	PR.PT-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

ISO-27001-2022	A.5.10
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

1.7.8 Ensure GDM autorun-never is enabled

Info

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

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

Solution

- IF - A user profile exists run the following command to set autorun-never to true for GDM users:

```
# gsettings set org.gnome.desktop.media-handling autorun-never true
```

Note:

- gsettings commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.

- The system must be restarted after all gsettings configurations have been set in order for CIS-CAT Assessor to appropriately assess.

- OR/IF - A user profile does not exist:

- create the file /etc/dconf/db/local.d/locks/00-media-autorun with the following content:

```
[org/gnome/desktop/media-handling] autorun-never=true <html:ol start="2"> - Update the systems databases:
```

```
# dconf update
```

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.8.7
800-171R3	03.08.07
800-53	MP-7
800-53R5	MP-7
CN-L3	8.5.4.1(c)
CSCV7	8.5
CSCV8	10.3
CSF	PR.PT-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

ISO-27001-2022	A.5.10
ISO-27001-2022	A.7.10
ISO/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
NESA	T1.4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

1.7.9 Ensure GDM autorun-never is not overridden

Info

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

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

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

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

Solution

- To prevent the user from overriding these settings, create the file `/etc/dconf/db/local.d/locks/00-media-autorun` with the following content:

[org/gnome/desktop/media-handling] autorun-never=true <html:ol start="2"> - Update the systems databases:

dconf update

Note:

- A user profile must exist in order to apply locks.
- Users must log out and back in again before the system-wide settings take effect.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.8.7
800-171R3	03.08.07
800-53	MP-7
800-53R5	MP-7
CN-L3	8.5.4.1(c)
CSCV7	8.5
CSCV8	10.3
CSF	PR.PT-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.7.10

ISO/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
NESA	T1.4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

1.7.10 Ensure XDMCP is not enabled

Info

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

XDMCP is inherently insecure.

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

Solution

Edit all files returned by the audit and remove or comment out the Enable=true line in the [xdmcp] block:

Example file:

```
# GDM configuration storage # # See /usr/share/gdm/gdm.schemas for a list of available options.
```

```
[daemon] # Uncomment the line below to force the login screen to use Xorg #WaylandEnable=false
```

```
# Enabling automatic login # AutomaticLoginEnable = true # AutomaticLogin = user1
```

```
# Enabling timed login # TimedLoginEnable = true # TimedLogin = user1 # TimedLoginDelay = 10
```

```
[security]
```

```
[xdmcp] # Enable=true <- **This line should be removed or commented out**
```

```
[chooser]
```

```
[debug] # Uncomment the line below to turn on debugging # More verbose logs # Additionally lets the X server dump core if it crashes #Enable=true
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7

CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

The command script with multiple lines returned :

Pass

2.1.1 Ensure autofs services are not in use

Info

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

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

Solution

Run the following commands to stop autofs.service and remove the autofs package:

```
# systemctl stop autofs.service # apt purge autofs
```

- OR -

- IF - the autofs package is required as a dependency:

Run the following commands to stop and mask autofs.service :

```
# systemctl stop autofs.service # systemctl mask autofs.service
```

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.

There may be packages that are dependent on the autofs package. If the autofs package is removed, these dependent packages will be removed as well. Before removing the autofs package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the autofs.service leaving the autofs package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.8.7
800-171R3	03.08.07
800-53	MP-7
800-53R5	MP-7
CN-L3	8.5.4.1(c)
CSCV7	8.5
CSCV8	10.3
CSF	PR.PT-2
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.7.10
ISO/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
NESA	T1.4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s autofs 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s autofs 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'autofs' is not installed and no information is available
```

2.1.2 Ensure avahi daemon services are not in use

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.

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

Solution

Run the following commands to stop avahi-daemon.socket and avahi-daemon.service and remove the avahi-daemon package:

```
# systemctl stop avahi-daemon.socket avahi-daemon.service # apt purge avahi-daemon
```

- OR -

- IF - the avahi-daemon package is required as a dependency:

Run the following commands to stop and mask the avahi-daemon.socket and avahi-daemon.service :

```
# systemctl stop avahi-daemon.socket avahi-daemon.service # systemctl mask avahi-daemon.socket avahi-daemon.service
```

Impact:

There may be packages that are dependent on the avahi package. If the avahi package is removed, these dependent packages will be removed as well. Before removing the avahi package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the avahi-daemon.socket and avahi-daemon.service leaving the avahi package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7

800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s avahi-daemon 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s avahi-daemon 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'avahi-daemon' is not installed and no information is available
```

2.1.3 Ensure dhcp server services are not in use

Info

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses. There are two versions of the DHCP protocol DHCPv4 and DHCPv6. At startup the server may be started for one or the other via the `-4` or `-6` arguments.

Unless a system is specifically set up to act as a DHCP server, it is recommended that this package be removed to reduce the potential attack surface.

Solution

Run the following commands to stop `isc-dhcp-server.service` and `isc-dhcp-server6.service` and remove the `isc-dhcp-server` package:

```
# systemctl stop isc-dhcp-server.service isc-dhcp-server6.service # apt purge isc-dhcp-server
```

- OR -

- IF - the `isc-dhcp-server` package is required as a dependency:

Run the following commands to stop and mask `isc-dhcp-server.service` and `isc-dhcp-server6.service` :

```
# systemctl stop isc-dhcp-server.service isc-dhcp-server6.service # systemctl mask isc-dhcp-server isc-dhcp-server6.service
```

Impact:

There may be packages that are dependent on the `isc-dhcp-server` package. If the `isc-dhcp-server` package is removed, these dependent packages will be removed as well. Before removing the `isc-dhcp-server` package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the `isc-dhcp-server.service` and `isc-dhcp-server6.service` leaving the `isc-dhcp-server` package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7

CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s isc-dhcp-server 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s isc-dhcp-server 2>&1 | /bin/grep -E '(^Status:|not installed)''
returned :

dpkg-query: package 'isc-dhcp-server' is not installed and no information is available
```

2.1.4 Ensure dns server services are not in use

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.

Note: bind9 is the package and bind.service is the alias for named.service

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 stop named.service and remove the bind9 package:

```
# systemctl stop named.service # apt purge bind9
```

- OR -

- IF - the bind9 package is required as a dependency:

Run the following commands to stop and mask bind9.service :

```
# systemctl stop named.service # systemctl mask named.service
```

Impact:

There may be packages that are dependent on the bind9 package. If the bind9 package is removed, these dependent packages will be removed as well. Before removing the bind9 package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask named.service leaving the bind9 package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8

CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s bind9 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s bind9 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'bind9' is not installed and no information is available
```

2.1.5 Ensure dnsmasq services are not in use

Info

dnsmasq is a lightweight tool that provides DNS caching, DNS forwarding and DHCP (Dynamic Host Configuration Protocol) services.

Unless a system is specifically designated to act as a DNS caching, DNS forwarding and/or DHCP server, it is recommended that the package be removed to reduce the potential attack surface.

Solution

Run the following commands to stop dnsmasq.service and remove dnsmasq package:

```
# systemctl stop dnsmasq.service # apt purge dnsmasq
```

- OR -

- IF - the dnsmasq package is required as a dependency:

Run the following commands to stop and mask the dnsmasq.service :

```
# systemctl stop dnsmasq.service # systemctl mask dnsmasq.service
```

Impact:

There may be packages that are dependent on the dnsmasq package. If the dnsmasq package is removed, these dependent packages will be removed as well. Before removing the dnsmasq package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the dnsmasq.service leaving the dnsmasq package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8

CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s dnsmasq 2>&1 | /bin/grep -E '^(Status:|not installed)'

expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s dnsmasq 2>&1 | /bin/grep -E '^(Status:|not installed)'' returned :
dpkg-query: package 'dnsmasq' is not installed and no information is available
```

2.1.6 Ensure ftp server services are not in use

Info

The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files. vsftpd is the Very Secure File Transfer Protocol Daemon.

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 commands to stop vsftpd.service and remove the vsftpd package:

```
# systemctl stop vsftpd.service # apt purge vsftpd
```

- OR -

- IF - the vsftpd package is required as a dependency:

Run the following commands to stop and mask the vsftpd.service :

```
# systemctl stop vsftpd.service # systemctl mask vsftpd.service
```

Note: Other ftp server packages may exist. If not required and authorized by local site policy, they should also be removed. If the package is required for a dependency, the service should be stopped and masked.

Impact:

There may be packages that are dependent on the vsftpd package. If the vsftpd package is removed, these dependent packages will be removed as well. Before removing the vsftpd package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the vsftpd.service leaving the vsftpd package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7

800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s vsftpd 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s vsftpd 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'vsftpd' is not installed and no information is available
```

2.1.7 Ensure ldap server services are not in use

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.

If the system will not need to act as an LDAP server, it is recommended that the software be removed to reduce the potential attack surface.

Solution

Run the following commands to stop slapd.service and remove the slapd package:

```
# systemctl stop slapd.service # apt purge slapd
```

- OR -

- IF - the slapd package is required as a dependency:

Run the following commands to stop and mask slapd.service :

```
# systemctl stop slapd.service # systemctl mask slapd.service
```

Impact:

There may be packages that are dependent on the slapd package. If the slapd package is removed, these dependent packages will be removed as well. Before removing the slapd package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the slapd.service leaving the slapd package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1

CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s slapd 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s slapd 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'slapd' is not installed and no information is available
```

2.1.8 Ensure message access server services are not in use

Info

dovecot-imapd and dovecot-pop3d are an open source IMAP and POP3 server for Linux based systems.

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

Note: Several IMAP/POP3 servers exist and can use other service names. These should also be audited and the packages removed if not required.

Solution

Run one of the following commands to remove dovecot-imapd and dovecot-pop3d :

Run the following commands to stop dovecot.socket and dovecot.service and remove the dovecot-imapd and dovecot-pop3d packages:

```
# systemctl stop dovecot.socket dovecot.service # apt purge dovecot-imapd dovecot-pop3d
```

- OR -

- IF - a package is installed and is required for dependencies:

Run the following commands to stop and mask dovecot.socket and dovecot.service :

```
# systemctl stop dovecot.socket dovecot.service # systemctl mask dovecot.socket dovecot.service
```

Impact:

There may be packages that are dependent on dovecot-imapd and/or dovecot-pop3d packages. If dovecot-imapd and dovecot-pop3d packages are removed, these dependent packages will be removed as well. Before removing dovecot-imapd and/or dovecot-pop3d packages, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask dovecot.socket and dovecot.service leaving dovecot-imapd and/or dovecot-pop3d packages installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7

800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - dovecot-pop3 not installed

The command '/bin/dpkg -s dovecot-pop3 2>&1 | /bin/grep -E '^(^Status:|not installed)'' returned :

dpkg-query: package 'dovecot-pop3' is not installed and no information is available

PASSED - dovecot-imapd not installed

The command '/bin/dpkg -s dovecot-imapd 2>&1 | /bin/grep -E '^(^Status:|not installed)'' returned :

dpkg-query: package 'dovecot-imapd' is not installed and no information is available

2.1.9 Ensure network file system services are not in use

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.

If the system does not export NFS shares, it is recommended that the nfs-kernel-server package be removed to reduce the remote attack surface.

Solution

Run the following command to stop nfs-server.service and remove nfs-kernel-server package:

```
# systemctl stop nfs-server.service # apt purge nfs-kernel-server
```

- OR -

- IF - the nfs-kernel-server package is required as a dependency:

Run the following commands to stop and mask the nfs-server.service :

```
# systemctl stop nfs-server.service # systemctl mask nfs-server.service
```

Impact:

There may be packages that are dependent on the nfs-kernel-server package. If the nfs-kernel-server package is removed, these dependent packages will be removed as well. Before removing the nfs-kernel-server package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the nfs-server.service leaving the nfs-kernel-server package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2

CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s nfs-kernel-server 2>&1 | /bin/grep -E '(^Status:|not installed)'

expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s nfs-kernel-server 2>&1 | /bin/grep -E '(^Status:|not installed)''
returned :

dpkg-query: package 'nfs-kernel-server' is not installed and no information is available
```

2.1.10 Ensure nis server services are not in use

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. The NIS client (ybind) was used to bind a machine to an NIS server and receive the distributed configuration files.

ypserv.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 ypserv.service be removed and other, more secure services be used

Solution

Run the following commands to stop ypserv.service and remove ypserv package:

```
# systemctl stop ypserv.service # apt purge ypserv
```

- OR -

- IF - the ypserv package is required as a dependency:

Run the following commands to stop and mask ypserv.service :

```
# systemctl stop ypserv.service # systemctl mask ypserv.service
```

Impact:

There may be packages that are dependent on the ypserv package. If the ypserv package is removed, these dependent packages will be removed as well. Before removing the ypserv package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the ypserv.service leaving the ypserv package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6

800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s ypserv 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s ypserv 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'ypserv' is not installed and no information is available
```

2.1.11 Ensure print server services are not in use

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.

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

Solution

Run the following commands to stop cups.socket and cups.service and remove the cups package:

```
# systemctl stop cups.socket cups.service # apt purge cups
```

- OR -

- IF - the cups package is required as a dependency:

Run the following commands to stop and mask the cups.socket and cups.service :

```
# systemctl stop cups.socket cups.service # systemctl mask cups.socket cups.service
```

Impact:

Removing the cups package, or disabling cups.socket and/or cups.service will prevent printing from the system, a common task for workstation systems.

There may be packages that are dependent on the cups package. If the cups package is removed, these dependent packages will be removed as well. Before removing the cups package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask cups.socket and cups.service leaving the cups package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6

800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s cups 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s cups 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'cups' is not installed and no information is available
```

2.1.12 Ensure rpcbind services are not in use

Info

The rpcbind utility maps RPC services to the ports on which they listen. RPC processes notify rpcbind when they start, registering the ports they are listening on and the RPC program numbers they expect to serve. The client system then contacts rpcbind on the server with a particular RPC program number. The rpcbind.service redirects the client to the proper port number so it can communicate with the requested service.

Portmapper is an RPC service, which always listens on tcp and udp 111, and is used to map other RPC services (such as nfs, nlockmgr, quotad, mountd, etc.) to their corresponding port number on the server. When a remote host makes an RPC call to that server, it first consults with portmap to determine where the RPC server is listening.

A small request (~82 bytes via UDP) sent to the Portmapper generates a large response (7x to 28x amplification), which makes it a suitable tool for DDoS attacks. If rpcbind is not required, it is recommended to remove rpcbind package to reduce the potential attack surface.

Solution

Run the following commands to stop rpcbind.socket and rpcbind.service and remove the rpcbind package:

```
# systemctl stop rpcbind.socket rpcbind.service # apt purge rpcbind
```

- OR -

- IF - the rpcbind package is required as a dependency:

Run the following commands to stop and mask the rpcbind.socket and rpcbind.service :

```
# systemctl stop rpcbind.socket rpcbind.service # systemctl mask rpcbind.socket rpcbind.service
```

Impact:

Many of the libvirt packages used by Enterprise Linux virtualization, and the nfs-utils package used for The Network File System (NFS), are dependent on the rpcbind package. If the rpcbind package is removed, these dependent packages will be removed as well. Before removing the rpcbind package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the rpcbind.socket and rpcbind.service leaving the rpcbind package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02

800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s rpcbind 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s rpcbind 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'rpcbind' is not installed and no information is available
```

2.1.13 Ensure rsync services are not in use

Info

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

rsync.service presents a security risk as the rsync protocol is unencrypted.

The rsync package should be removed to reduce the attack area of the system.

Solution

Run the following commands to stop rsync.service and remove the rsync package:

```
# systemctl stop rsync.service # apt purge rsync
```

- OR -

- IF - the rsync package is required as a dependency:

Run the following commands to stop and mask rsync.service :

```
# systemctl stop rsync.service # systemctl mask rsync.service
```

Impact:

There may be packages that are dependent on the rsync package. If the rsync package is removed, these dependent packages will be removed as well. Before removing the rsync package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask rsync.service leaving the rsync package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1

CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - rsync not active

The command '/bin/systemctl is-active rsync.service 2>/dev/null | /bin/grep '^active' | /bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}' returned :

pass

PASSED - rsync not enabled

The command '/bin/systemctl is-enabled rsync.service 2>/dev/null | /bin/grep '^enabled' | /bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}' returned :

pass

2.1.14 Ensure samba file server services are not in use

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.

If there is no need to mount directories and file systems to Windows systems, then this service should be deleted to reduce the potential attack surface.

Solution

Run the following commands to stop smbd.service and remove samba package:

```
# systemctl stop smbd.service # apt purge samba
```

- OR -

- IF - the samba package is required as a dependency:

Run the following commands to stop and mask the smbd.service :

```
# systemctl stop smbd.service # systemctl mask smbd.service
```

Impact:

There may be packages that are dependent on the samba package. If the samba package is removed, these dependent packages will be removed as well. Before removing the samba package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the smbd.service leaving the samba package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2

CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s samba 2>&1 | /bin/grep -E '(^Status:|not installed)'

expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s samba 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'samba' is not installed and no information is available
```

2.1.15 Ensure snmp services are not in use

Info

Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment, computer equipment and devices like UPSs.

Net-SNMP is a suite of applications used to implement SNMPv1 (RFC 1157), SNMPv2 (RFCs 1901-1908), and SNMPv3 (RFCs 3411-3418) using both IPv4 and IPv6.

Support for SNMPv2 classic (a.k.a. "SNMPv2 historic" - RFCs 1441-1452) was dropped with the 4.0 release of the UCD-snmp package.

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

The SNMP server can communicate using SNMPv1 which transmits data in the clear and does not require authentication to execute commands. SNMPv3 replaces the simple/clear text password sharing used in SNMPv2 with more securely encoded parameters. If the the SNMP service is not required, the snmpd package should be removed to reduce the attack surface of the system.

Note: If SNMP is required:

- The server should be configured for SNMP v3 only. User Authentication and Message Encryption should be configured.
- If SNMP v2 is absolutely necessary, modify the community strings' values.

Solution

Run the following commands to stop snmpd.service and remove the snmpd package:

```
# systemctl stop snmpd.service # apt purge snmpd
```

- OR - If the package is required for dependencies:

Run the following commands to stop and mask the snmpd.service :

```
# systemctl stop snmpd.service # systemctl mask snmpd.service
```

Impact:

There may be packages that are dependent on the snmpd package. If the snmpd package is removed, these packages will be removed as well.

Before removing the snmpd package, review any dependent packages to determine if they are required on the system. If a dependent package is required, stop and mask the snmpd.service leaving the snmpd package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s snmpd 2>&1 | /bin/grep -E '(^Status:|not installed)'
expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s snmpd 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :  
dpkg-query: package 'snmpd' is not installed and no information is available
```

2.1.16 Ensure tftp server services are not in use

Info

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files.

Unless there is a need to run the system as a TFTP server, it is recommended that the package be removed to reduce the potential attack surface.

TFTP does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to exploit TFTP to gain access to files

Solution

Run the following commands to stop tftpd-hpa.service and remove the tftpd-hpa package:

```
# systemctl stop tftpd-hpa.service # apt purge tftpd-hpa
```

- OR -

- IF - the tftpd-hpa package is required as a dependency:

Run the following commands to stop and mask tftpd-hpa.service :

```
# systemctl stop tftpd-hpa.service # systemctl mask tftpd-hpa.service
```

Impact:

TFTP is often used to provide files for network booting such as for PXE based installation of servers.

There may be packages that are dependent on the tftpd-hpa package. If the tftpd-hpa package is removed, these dependent packages will be removed as well. Before removing the tftpd-hpa package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask tftpd-hpa.service leaving the tftpd-hpa package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6

800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s tftpd-hpa 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s tftpd-hpa 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'tftpd-hpa' is not installed and no information is available
```

2.1.17 Ensure web proxy server services are not in use

Info

Squid is a standard proxy server used in many distributions and environments.

Unless a system is specifically set up to act as a proxy server, it is recommended that the squid package be removed to reduce the potential attack surface.

Note: Several HTTP proxy servers exist. These should be checked and removed unless required.

Solution

Run the following commands to stop squid.service and remove the squid package:

```
# systemctl stop squid.service # apt purge squid
```

- OR - If the squid package is required as a dependency:

Run the following commands to stop and mask the squid.service :

```
# systemctl stop squid.service # systemctl mask squid.service
```

Impact:

There may be packages that are dependent on the squid package. If the squid package is removed, these dependent packages will be removed as well. Before removing the squid package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the squid.service leaving the squid package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3

CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s squid 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s squid 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'squid' is not installed and no information is available
```

2.1.19 Ensure xinetd services are not in use

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.

If there are no xinetd services required, it is recommended that the package be removed to reduce the attack surface of the system.

Note: If an xinetd service or services are required, ensure that any xinetd service not required is stopped and masked

Solution

Run the following commands to stop xinetd.service and remove the xinetd package:

```
# systemctl stop xinetd.service # apt purge xinetd
```

-OR-

-IF- the xinetd package is required as a dependency:

Run the following commands to stop and mask the xinetd.service :

```
# systemctl stop xinetd.service # systemctl mask xinetd.service
```

Impact:

There may be packages that are dependent on the xinetd package. If the xinetd package is removed, these dependent packages will be removed as well. Before removing the xinetd package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask xinetd.service leaving the xinetd package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7

CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s xinetd 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s xinetd 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'xinetd' is not installed and no information is available
```

2.1.21 Ensure mail transfer agent is configured for local-only mode

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.

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/postfix/main.cf` and add the following line to the RECEIVING MAIL section. If the line already exists, change it to look like the line below:

```
inet_interfaces = loopback-only
```

Run the following command to restart postfix :

```
# systemctl restart postfix
```

Note:

- This recommendation is designed around the postfix mail server.
- Depending on your environment you may have an alternative MTA installed such as exim4. If this is the case consult the documentation for your installed MTA to configure the recommended state.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3

CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?:i)^\s**\s**pass:?\s***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- Port "25" is not listening on a non-loopback network interface
- Port "465" is not listening on a non-loopback network interface
- Port "587" is not listening on a non-loopback network interface
- MTA is not bound to a non loopback network interface
  "inet_interfaces = loopback-only"
```

2.2.1 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.

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/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	2.6
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9

ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s nis 2>&1 | /bin/grep -E '(^Status:|not installed)'

expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s nis 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :  
dpkg-query: package 'nis' is not installed and no information is available
```

2.2.2 Ensure rsh client is not installed

Info

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

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

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/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9

ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s rsh-client 2>&1 | /bin/grep -E '(^Status:|not installed)'

expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s rsh-client 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :  
dpkg-query: package 'rsh-client' is not installed and no information is available
```

2.2.3 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.

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/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7

LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s talk 2>&1 | /bin/grep -E '(^Status:|not installed)'

expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s talk 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :  
dpkg-query: package 'talk' is not installed and no information is available
```

2.2.4 Ensure telnet client is not installed

Info

The inetutils-telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol.

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

Run the following commands to uninstall telnet & inetutils-telnet :

```
# apt purge telnet # apt purge inetutils-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/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9

ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

```
-----
PASSED - Ensure package name equals 'inetutils-telnet' is not installed
The command '/bin/dpkg -s inetutils-telnet 2>&1 | /bin/grep -E '^(Status:|not installed)''
returned :

dpkg-query: package 'inetutils-telnet' is not installed and no information is available

-----
PASSED - Ensure package name equals 'telnet' is not installed
The command '/bin/dpkg -s telnet 2>&1 | /bin/grep -E '^(Status:|not installed)'' returned :

dpkg-query: package 'telnet' is not installed and no information is available
```

2.2.5 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.

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.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A

NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s ldap-utils 2>&1 | /bin/grep -E '(^Status:|not installed)'

expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s ldap-utils 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :  
dpkg-query: package 'ldap-utils' is not installed and no information is available
```

2.2.6 Ensure ftp client is not installed

Info

tnftp an enhanced FTP client, is the user interface to the Internet standard File Transfer Protocol. The program allows a user to transfer files to and from a remote network site.

Unless there is a need to run the system using Internet standard File Transfer Protocol (for example, to allow anonymous downloads), it is recommended that the package be removed to reduce the potential attack surface.

Solution

Run the following commands to uninstall tnftp & ftp :

```
# apt purge ftp # apt purge tnftp
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - Ensure package name equals 'ftp' is not installed

The command '/bin/dpkg -s ftp 2>&1 | /bin/grep -E '^(Status:|not installed)'' returned :

dpkg-query: package 'ftp' is not installed and no information is available

PASSED - Ensure package name equals 'tnftp' is not installed

The command '/bin/dpkg -s tnftp 2>&1 | /bin/grep -E '^(Status:|not installed)'' returned :

dpkg-query: package 'tnftp' is not installed and no information is available

2.3.1.1 Ensure a single time synchronization daemon 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.

Note:

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

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

Solution

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

Select one of the two time synchronization daemons; chrony (1) or systemd-timesyncd (2) and following the remediation procedure for the selected daemon.

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

- chrony

Run the following command to install chrony :

```
# apt install chrony
```

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

```
# systemctl stop systemd-timesyncd.service
```

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

Note:

- Subsection:

Configure chrony

should be followed

- Subsection:

Configure systemd-timesyncd

should be skipped

<xhtml:ol start="2"> - systemd-timesyncd

Run the following command to remove the chrony package:

apt purge chrony # apt autoremove chrony

Note:

- Subsection:

Configure systemd-timesyncd

should be followed

- Subsection:

Configure chrony

should be skipped

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.6
800-171	3.3.7
800-171R3	03.03.06a.
800-171R3	03.03.07
800-53	AU-7
800-53	AU-8
800-53R5	AU-7
800-53R5	AU-8
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSCV8	8.4
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.17
ITSG-33	AU-7
ITSG-33	AU-8
LEVEL	1A
NESA	T3.6.2

QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4
TBA-FIISB	37.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?:i)^\[s]*\[s]*pass:?\[s]*\[s]*\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- Only one time sync daemon is in use on the system
- Daemon: "systemd-timesyncd.service" is enabled on the system
- Daemon: "systemd-timesyncd.service" is active on the system
- Daemon: "chrony.service" is not enabled and not active on the system
```

2.3.2.1 Ensure systemd-timesyncd configured with authorized timeserver

Info

NTP=

- A space-separated list of NTP server host names or IP addresses. During runtime this list is combined with any per-interface NTP servers acquired from `systemd-networkd.service(8)`. `systemd-timesyncd` will contact all configured system or per-interface servers in turn, until one responds. When the empty string is assigned, the list of NTP servers is reset, and all prior assignments will have no effect. This setting defaults to an empty list.

FallbackNTP=

- A space-separated list of NTP server host names or IP addresses to be used as the fallback NTP servers. Any per-interface NTP servers obtained from `systemd-networkd.service(8)` take precedence over this setting, as do any servers set via `NTP=` above. This setting is hence only relevant if no other NTP server information is known. When the empty string is assigned, the list of NTP servers is reset, and all prior assignments will have no effect. If this option is not given, a compiled-in list of NTP servers is used.

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Solution

Set NTP and/or FallbackNTP parameters to local site approved authoritative time server(s) in `/etc/systemd/timesyncd.conf` or a file in `/etc/systemd/timesyncd.conf.d/` ending in `inconf` in the `[Time]` section:

Example file:

```
[Time] NTP=time.nist.gov # Uses the generic name for NIST's time servers FallbackNTP=time-a-g.nist.gov
time-b-g.nist.gov time-c-g.nist.gov # Space separated list of NIST time servers
```

Example script to create systemd drop-in configuration file:

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

```
{ a_settings=("NTP=time.nist.gov" "FallbackNTP=time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov") [ ! -
d /etc/systemd/timesyncd.conf.d/ ] && mkdir /etc/systemd/timesyncd.conf.d/ if grep -Psq -- '^h*[Time]' /
etc/systemd/timesyncd.conf.d/60-timesyncd.conf; then printf '%s ' "" "${a_settings[@]}" >> /etc/systemd/
timesyncd.conf.d/60-timesyncd.conf else printf '%s ' "" "[Time]" "${a_settings[@]}" >> /etc/systemd/
timesyncd.conf.d/60-timesyncd.conf fi }
```

Note: If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run to following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.6
800-171	3.3.7
800-171R3	03.03.06a.
800-171R3	03.03.07
800-53	AU-7
800-53	AU-8
800-53R5	AU-7
800-53R5	AU-8
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSCV8	8.4
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.17
ITSG-33	AU-7
ITSG-33	AU-8
LEVEL	1A
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4
TBA-FIISB	37.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***[s]*pass:[s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- "NTP" is correctly set to "time.nist.gov"
  in "/etc/systemd/timesyncd.conf"
- "FallbackNTP" is correctly set to "time-a-g.nist.gov"
  in "/etc/systemd/timesyncd.conf"
```

2.3.2.2 Ensure systemd-timesyncd is enabled and running

Info

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network

systemd-timesyncd needs to be enabled and running in order to synchronize the system to a timeserver.

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Solution

- IF - systemd-timesyncd is in use on the system, run the following commands:

Run the following command to unmask systemd-timesyncd.service :

```
# systemctl unmask systemd-timesyncd.service
```

Run the following command to enable and start systemd-timesyncd.service :

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

- OR -

If another time synchronization service is in use on the system, run the following command to stop and mask systemd-timesyncd :

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.6
800-171	3.3.7
800-171R3	03.03.06a.
800-171R3	03.03.07
800-53	AU-7
800-53	AU-8
800-53R5	AU-7
800-53R5	AU-8
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSCV8	8.4
CSF	PR.PT-1

CSF	RS.AN-3
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.17
ITSG-33	AU-7
ITSG-33	AU-8
LEVEL	1A
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4
TBA-FIISB	37.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - check if systemd-timesyncd is active

The command '/bin/systemctl is-active systemd-timesyncd.service' returned :

active

PASSED - systemctl is-enabled systemd-timesyncd.service

The command '/bin/systemctl is-enabled systemd-timesyncd.service' returned :

enabled

2.3.3.1 Ensure chrony is configured with authorized timeserver

Info

-

server

- The server directive specifies an NTP server which can be used as a time source. The client-server relationship is strictly hierarchical: a client might synchronize its system time to that of the server, but the server's system time will never be influenced by that of a client.
- This directive can be used multiple times to specify multiple servers.
- The directive is immediately followed by either the name of the server, or its IP address.

-

pool

- The syntax of this directive is similar to that for the server directive, except that it is used to specify a pool of NTP servers rather than a single NTP server. The pool name is expected to resolve to multiple addresses which might change over time.
- This directive can be used multiple times to specify multiple pools.
- All options valid in the server directive can be used in this directive too.

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Solution

Edit /etc/chrony/chrony.conf or a file ending insources in /etc/chrony/sources.d/ and add or edit server or pool lines as appropriate according to local site policy:

Edit the Chrony configuration and add or edit the server and/or pool lines returned by the Audit Procedure as appropriate according to local site policy

<[server | pool]> <[remote-server | remote-pool]>

Example script to add a drop-in configuration for the pool directive:

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

```
{ [ ! -d "/etc/chrony/sources.d/" ] && mkdir /etc/chrony/sources.d/ printf '%s ' "" "#The maxsources option is unique to the pool directive" "pool time.nist.gov iburst maxsources 4" >> /etc/chrony/sources.d/60-sources.sources chronyc reload sources &>/dev/null }
```

Example script to add a drop-in configuration for the server directive:

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

```
{ [ ! -d "/etc/chrony/sources.d/" ] && mkdir /etc/chrony/sources.d/ printf '%s ' "" "server time-a-g.nist.gov iburst" "server 132.163.97.3 iburst" "server time-d-b.nist.gov iburst" >> /etc/chrony/sources.d/60-sources.sources chronyc reload sources &>/dev/null }
```

Run the following command to reload the chronyd config:

systemctl reload-or-restart chronyd

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.6
800-171	3.3.7
800-171R3	03.03.06a.
800-171R3	03.03.07
800-53	AU-7
800-53	AU-8
800-53R5	AU-7
800-53R5	AU-8
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSCV8	8.4
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.17
ITSG-33	AU-7
ITSG-33	AU-8
LEVEL	1A
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4
TBA-FIISB	37.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

2.3.3.2 Ensure chrony is running as user _chrony

Info

The chrony package is installed with a dedicated user account _chrony This account is granted the access required by the chronyd service

The chronyd service should run with only the required privlidges

Solution

Add or edit the user line to /etc/chrony/chrony.conf or a file ending inconf in /etc/chrony/conf.d/ :

user _chrony

- OR -

If another time synchronization service is in use on the system, run the following command to remove chrony from the system:

apt purge chrony # apt autoremove chrony

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.6
800-171	3.3.7
800-171R3	03.03.06a.
800-171R3	03.03.07
800-53	AU-7
800-53	AU-8
800-53R5	AU-7
800-53R5	AU-8
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSCV8	8.4
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.17
ITSG-33	AU-7
ITSG-33	AU-8
LEVEL	1A
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4
TBA-FIISB	37.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

2.3.3.3 Ensure chrony is enabled and running

Info

chrony is a daemon for synchronizing the system clock across the network

chrony needs to be enabled and running in order to synchronize the system to a timeserver.

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

Solution

- IF - chrony is in use on the system, run the following commands:

Run the following command to unmask chrony.service :

```
# systemctl unmask chrony.service
```

Run the following command to enable and start chrony.service :

```
# systemctl --now enable chrony.service
```

- OR -

If another time synchronization service is in use on the system, run the following command to remove chrony :

```
# apt purge chrony # apt autoremove chrony
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.6
800-171	3.3.7
800-171R3	03.03.06a.
800-171R3	03.03.07
800-53	AU-7
800-53	AU-8
800-53R5	AU-7
800-53R5	AU-8
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSCV8	8.4
CSF	PR.PT-1
CSF	RS.AN-3

CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.17
ITSG-33	AU-7
ITSG-33	AU-8
LEVEL	1A
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4
TBA-FIISB	37.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

2.4.1.1 Ensure cron daemon is enabled and active

Info

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

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

- IF - cron is installed on the system:

Run the following commands to unmask, enable, and start cron :

```
# systemctl unmask "$(systemctl list-unit-files | awk '$1~/^cron?.service/{print $1}')"
# systemctl --now enable "$(systemctl list-unit-files | awk '$1~/^cron?.service/{print $1}')
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
LEVEL	1A
NESA	T3.2.1
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

192.168.40.171

```
All of the following must pass to satisfy this requirement:
```

```
-----
```

```
PASSED - enabled
```

```
The command '/bin/systemctl list-unit-files | /bin/awk '$1~/^crond?\.service/{print $2}''  
returned :
```

```
enabled
```

```
-----
```

```
PASSED - active
```

```
The command '/bin/systemctl list-units | /bin/awk '$1~/^crond?\.service/{print $3}'' returned :
```

```
active
```


2.4.1.2 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.

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

- IF - cron is installed on the system:

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/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)

CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1

NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/crontab group: root mask: 177 owner: root

Hosts

192.168.40.171

```
The file /etc/crontab with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven
permissions : FALSE is compliant with the policy value
```

```
/etc/crontab
```

2.4.1.3 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.

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

- IF - cron is installed on the system:

Run the following commands to set ownership and permissions on the /etc/cron.hourly directory:

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)

CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1

NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/cron.hourly group: root mask: 077 owner: root

Hosts

192.168.40.171

```
The file /etc/cron.hourly with fmode owner: root group: root mode: 0700 uid: 0 gid: 0 uneven
permissions : FALSE is compliant with the policy value
```

```
/etc/cron.hourly
```

2.4.1.4 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.

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

- IF - cron is installed on the system:

Run the following commands to set ownership and permissions on the /etc/cron.daily directory:

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)

CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1

NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/cron.daily group: root mask: 077 owner: root

Hosts

192.168.40.171

```
The file /etc/cron.daily with fmode owner: root group: root mode: 0700 uid: 0 gid: 0 uneven
permissions : FALSE is compliant with the policy value
```

```
/etc/cron.daily
```

2.4.1.5 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.

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

- IF - cron is installed on the system:

Run the following commands to set ownership and permissions on the /etc/cron.weekly directory:

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)

CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1

NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/cron.weekly group: root mask: 077 owner: root

Hosts

192.168.40.171

```
The file /etc/cron.weekly with fmode owner: root group: root mode: 0700 uid: 0 gid: 0 uneven
permissions : FALSE is compliant with the policy value
```

```
/etc/cron.weekly
```

2.4.1.6 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.

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

- IF - cron is installed on the system:

Run the following commands to set ownership and permissions on the /etc/cron.monthly directory:

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)

CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1

NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/cron.monthly group: root mask: 077 owner: root

Hosts

192.168.40.171

```
The file /etc/cron.monthly with fmode owner: root group: root mode: 0700 uid: 0 gid: 0 uneven
permissions : FALSE is compliant with the policy value
```

```
/etc/cron.monthly
```

2.4.1.7 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.

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

- IF - cron is installed on the system:

Run the following commands to set ownership and permissions on the /etc/cron.d directory:

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/cron.d group: root mask: 077 owner: root

Hosts

192.168.40.171

```
The file /etc/cron.d with fmode owner: root group: root mode: 0700 uid: 0 gid: 0 uneven
permissions : FALSE is compliant with the policy value
```

```
/etc/cron.d
```

2.4.1.8 Ensure crontab is restricted to authorized users

Info

crontab is the program used to install, deinstall, or list the tables used to drive the cron daemon. Each user can have their own crontab, and though these are files in `/var/spool/cron/crontabs` they are not intended to be edited directly.

If the `/etc/cron.allow` file exists, then you must be listed (one user per line) therein in order to be allowed to use this command. If the `/etc/cron.allow` file does not exist but the `/etc/cron.deny` file does exist, then you must not be listed in the `/etc/cron.deny` file in order to use this command.

If neither of these files exists, then depending on site-dependent configuration parameters, only the super user will be allowed to use this command, or all users will be able to use this command.

If both files exist then `/etc/cron.allow` takes precedence. Which means that `/etc/cron.deny` is not considered and your user must be listed in `/etc/cron.allow` in order to be able to use the crontab.

Regardless of the existence of any of these files, the root administrative user is always allowed to setup a crontab.

The files `/etc/cron.allow` and `/etc/cron.deny` if they exist, must be either world-readable, or readable by group crontab. If they are not, then cron will deny access to all users until the permissions are fixed.

There is one file for each user's crontab under the `/var/spool/cron/crontabs` directory. Users are not allowed to edit the files under that directory directly to ensure that only users allowed by the system to run periodic tasks can add them, and only syntactically correct crontabs will be written there. This is enforced by having the directory writable only by the crontab group and configuring crontab command with the `setgid` bit set for that specific group.

Note:

- Even though a given user is not listed in `cron.allow` cron jobs can still be run as that user
- The files `/etc/cron.allow` and `/etc/cron.deny` if they exist, only controls administrative access to the crontab command for scheduling and modifying cron jobs

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

- IF - cron is installed on the system:

Run the following script to:

- Create `/etc/cron.allow` if it doesn't exist
- Change owner to user root
- Change group owner to group root - OR - group crontab if it exists
- Change mode to 640 or more restrictive

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

```
{ [ ! -e "/etc/cron.deny" ] && touch /etc/cron.allow chmod u-x,g-wx,o-rwx /etc/cron.allow if grep -Pq -- '^h*cronab:' /etc/group; then chown root:cronab /etc/cron.allow else chown root:root /etc/cron.allow fi }
```

- IF - /etc/cron.deny exists, run the following script to:

- Change owner to user root
- Change group owner to group root - OR - group cronab if it exists
- Change mode to 640 or more restrictive

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

```
{ if [ -e "/etc/cron.deny" ]; then chmod u-x,g-wx,o-rwx /etc/cron.deny if grep -Pq -- '^h*cronab:' /etc/group; then chown root:cronab /etc/cron.deny else chown root:root /etc/cron.deny fi fi }
```

Note: On systems where cron is configured to use the group cronab if the group cronab is not set as the owner of cron.allow then cron will deny access to all users and you will see an error similar to:

You (<USERNAME>) are not allowed to use this program (cronab) See cronab(1) for more information

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)

CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - /etc/cron.allow file permissions

The file /etc/cron.allow with fmode owner: root group: root mode: 0640 uid: 0 gid: 0 uneven permissions : FALSE is compliant with the policy value

/etc/cron.allow

PASSED - /etc/cron.deny file permissions

The file /etc/cron.deny with fmode owner: root group: root mode: 0640 uid: 0 gid: 0 uneven permissions : FALSE is compliant with the policy value

/etc/cron.deny

2.4.2.1 Ensure at is restricted to authorized users

Info

at allows fairly complex time specifications, extending the POSIX.2 standard. It accepts times of the form HH:MM to run a job at a specific time of day. (If that time is already past, the next day is assumed.) You may also specify midnight, noon, or teatime (4pm) and you can have a time-of-day suffixed with AM or PM for running in the morning or the evening. You can also say what day the job will be run, by giving a date in the form month-name day with an optional year, or giving a date of the form MMDD[CC]YY, MM/DD/[CC]YY, DD.MM.[CC]YY or [CC]YY-MM-DD. The specification of a date must follow the specification of the time of day. You can also give times like now + count time-units, where the time-units can be minutes, hours, days, or weeks and you can tell at to run the job today by suffixing the time with today and to run the job tomorrow by suffixing the time with tomorrow.

The /etc/at.allow and /etc/at.deny files determine which user can submit commands for later execution via at or batch. The format of the files is a list of usernames, one on each line. Whitespace is not permitted. If the file /etc/at.allow exists, only usernames mentioned in it are allowed to use at. If /etc/at.allow does not exist, /etc/at.deny is checked, every username not mentioned in it is then allowed to use at. An empty /etc/at.deny means that every user may use at. If neither file exists, only the superuser is allowed to use at.

On many systems, only the system administrator is authorized to schedule at jobs. Using the at.allow file to control who can run at jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Solution

- IF - at is installed on the system:

Run the following script to:

- /etc/at.allow :
- Create the file if it doesn't exist
- Change owner or user root
- If group daemon exists, change to group daemon else change group to root
- Change mode to 640 or more restrictive
- - IF - /etc/at.deny exists:
- Change owner or user root
- If group daemon exists, change to group daemon else change group to root
- Change mode to 640 or more restrictive

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

```
{ grep -Pq -- '^daemonb' /etc/group && |_group="daemon" || |_group="root"
[ ! -e "/etc/at.allow" ] && touch /etc/at.allow chown root:"$_group" /etc/at.allow chmod u-x,g-wx,o-rwx /etc/at.allow [ -e "/etc/at.deny" ] && chown root:"$_group" /etc/at.deny [ -e "/etc/at.deny" ] && chmod u-x,g-wx,o-rwx /etc/at.deny }
```

See Also

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3

ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2

QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

3.1.2 Ensure wireless interfaces are disabled

Info

Wireless networking is used when wired networks are unavailable.

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

Solution

Run the following script to disable any wireless interfaces:

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

```
{ module_fix() { if ! modprobe -n -v "$l_mname" | grep -P -- '^h*install /bin/(true|false)'; then echo -e " -  
setting module: \"$l_mname\" to be un-loadable"
```

```
echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mname".conf fi if lsmod | grep "$l_mname"  
> /dev/null 2>&1; then echo -e " - unloading module \"$l_mname\""
```

```
modprobe -r "$l_mname"
```

```
fi if ! grep -Pq -- "^h*blacklist+$l_mnameb" /etc/modprobe.d/*; then echo -e " - deny listing \"$l_mname\""
```

```
echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mname".conf fi } if [ -n "$(find /sys/class/net/* -type  
d -name wireless)" ]; then l_dname=$(for driverdir in $(find /sys/class/net/* -type d -name wireless | xargs  
-0 dirname); do basename "$(readlink -f "$driverdir/device/driver/module)";done | sort -u) for l_mname in  
$l_dname; do module_fix done fi }
```

Impact:

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	15.4
CSCV7	15.5
CSCV8	4.8

CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s**\s**pass:?\s***\$ timeout: 7200

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **

- System has no wireless NICs installed
```

3.1.3 Ensure bluetooth services are not in use

Info

Bluetooth is a short-range wireless technology standard that is used for exchanging data between devices over short distances. It employs UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz. It is mainly used as an alternative to wire connections.

An attacker may be able to find a way to access or corrupt your data. One example of this type of activity is bluesnarfing which refers to attackers using a Bluetooth connection to steal information off of your Bluetooth device. Also, viruses or other malicious code can take advantage of Bluetooth technology to infect other devices. If you are infected, your data may be corrupted, compromised, stolen, or lost.

Solution

Run the following commands to stop bluetooth.service and remove the bluez package:

```
# systemctl stop bluetooth.service # apt purge bluez
```

- OR -

- IF - the bluez package is required as a dependency:

Run the following commands to stop and mask bluetooth.service :

```
# systemctl stop bluetooth.service # systemctl mask bluetooth.service
```

Note: A reboot may be required

Impact:

Many personal electronic devices (PEDs) use Bluetooth technology. For example, you may be able to operate your computer with a wireless keyboard. Disabling Bluetooth will prevent these devices from connecting to the system.

There may be packages that are dependent on the bluez package. If the bluez package is removed, these dependent packages will be removed as well. Before removing the bluez package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask bluetooth.service leaving the bluez package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06

800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s bluez 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s bluez 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :
dpkg-query: package 'bluez' is not installed and no information is available
```

3.3.1 Ensure ip forwarding is disabled

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.

Setting `net.ipv4.ip_forward` and `net.ipv6.conf.all.forwarding` to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Solution

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

- `net.ipv4.ip_forward = 0`

Example:

```
# printf '%s ' "net.ipv4.ip_forward = 0" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

- IF - IPv6 is enabled on the system:

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

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

Example:

```
# printf '%s ' "net.ipv6.conf.all.forwarding = 0" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

```
{ sysctl -w net.ipv6.conf.all.forwarding=0 sysctl -w net.ipv6.route.flush=1 }
```

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

Impact:

IP forwarding is required on systems configured to act as a router. If these parameters are disabled, the system will not be able to perform as a router.

Many Cloud Service Provider (CSP) hosted systems require IP forwarding to be enabled. If the system is running on a CSP platform, this requirement should be reviewed before disabling IP forwarding.

See Also

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?!)[\s]***[\s]*pass:[\s]***\$

Hosts

192.168.40.171

```
The command script with multiple lines returned :

sysctl: cannot stat /proc/sys/net/ipv6/conf/all/disable_ipv6: No such file or directory

- Audit Result:
  ** PASS **
- "net.ipv4.ip_forward" is correctly set to "0"
```


- in the running configuration
- "net.ipv4.ip_forward" is correctly set to "0"
in "/etc/sysctl.conf"
- IPv6 is disabled on the system, "net.ipv6.conf.all.forwarding" is not applicable

3.3.2 Ensure packet redirect sending is disabled

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.

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 file in `/etc/sysctl.d/` ending in `conf` :

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

Example:

```
# printf '%s ' "net.ipv4.conf.all.send_redirects = 0" "net.ipv4.conf.default.send_redirects = 0" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

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

Impact:

IP forwarding is required on systems configured to act as a router. If these parameters are disabled, the system will not be able to perform as a router.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7

800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?!)[\s]***[\s]*pass:[\s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- "net.ipv4.conf.all.send_redirects" is correctly set to "0"
  in the running configuration
- "net.ipv4.conf.all.send_redirects" is correctly set to "0"
  in "/etc/sysctl.conf"
- "net.ipv4.conf.default.send_redirects" is correctly set to "0"
  in the running configuration
- "net.ipv4.conf.default.send_redirects" is correctly set to "0"
  in "/etc/sysctl.conf"
```

3.3.3 Ensure bogus icmp responses are ignored

Info

Setting `net.ipv4.icmp_ignore_bogus_error_responses` to 1 prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast retransmits, keeping file systems from filling up with useless log messages.

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 file in `/etc/sysctl.d/` ending in `conf` :

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

Example:

```
# printf '%s ' "net.ipv4.icmp_ignore_bogus_error_responses = 1" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3

CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s***\s**pass:?\s***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- "net.ipv4.icmp_ignore_bogus_error_responses" is correctly set to "1"
  in the running configuration
- "net.ipv4.icmp_ignore_bogus_error_responses" is correctly set to "1"
  in "/etc/ufw/sysctl.conf"
```

3.3.4 Ensure broadcast icmp requests are ignored

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.

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

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

Example:

```
# printf '%s ' "net.ipv4.icmp_echo_ignore_broadcasts = 1" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8

CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s***\s**pass:?\s***\\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- "net.ipv4.icmp_echo_ignore_broadcasts" is correctly set to "1"
  in the running configuration
- "net.ipv4.icmp_echo_ignore_broadcasts" is correctly set to "1"
  in "/etc/ufw/sysctl.conf"
```

3.3.5 Ensure icmp redirects are not accepted

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.

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

Solution

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

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

Example:

```
# printf '%s ' "net.ipv4.conf.all.accept_redirects = 0" "net.ipv4.conf.default.accept_redirects = 0" >> /etc/
sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

- IF - IPv6 is enabled on the system:

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

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

Example:

```
# printf '%s ' "net.ipv6.conf.all.accept_redirects = 0" "net.ipv6.conf.default.accept_redirects = 0" >> /etc/
sysctl.d/60-netipv6_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***[s]*pass:[s]***\$

Hosts

192.168.40.171

```
The command script with multiple lines returned :  
  
sysctl: cannot stat /proc/sys/net/ipv6/conf/all/disable_ipv6: No such file or directory
```

```
- Audit Result:
  ** PASS **
- "net.ipv4.conf.all.accept_redirects" is correctly set to "0"
  in the running configuration
- "net.ipv4.conf.all.accept_redirects" is correctly set to "0"
  in "/etc/ufw/sysctl.conf"
- "net.ipv4.conf.default.accept_redirects" is correctly set to "0"
  in the running configuration
- "net.ipv4.conf.default.accept_redirects" is correctly set to "0"
  in "/etc/ufw/sysctl.conf"
- IPv6 is disabled on the system, "net.ipv6.conf.all.accept_redirects" is not applicable
- IPv6 is disabled on the system, "net.ipv6.conf.default.accept_redirects" is not applicable
```

3.3.6 Ensure secure icmp redirects are not accepted

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.

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

Solution

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

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

Example:

```
# printf '%s ' "net.ipv4.conf.all.secure_redirects = 0" "net.ipv4.conf.default.secure_redirects = 0" >> /etc/
sysctl.d/60-netip4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2

CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s**\s**pass:?\s***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- "net.ipv4.conf.all.secure_redirects" is correctly set to "0"
  in the running configuration
- "net.ipv4.conf.all.secure_redirects" is correctly set to "0"
  in "/etc/sysctl.conf"
- "net.ipv4.conf.default.secure_redirects" is correctly set to "0"
  in the running configuration
- "net.ipv4.conf.default.secure_redirects" is correctly set to "0"
  in "/etc/sysctl.conf"
```

3.3.7 Ensure reverse path filtering is enabled

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).

Setting `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` to 1 is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Solution

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

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

Example:

```
# printf '%s ' "net.ipv4.conf.all.rp_filter = 1" "net.ipv4.conf.default.rp_filter = 1" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

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

Impact:

If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02

800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s**\s**pass:[\s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- "net.ipv4.conf.all.rp_filter" is correctly set to "1"
  in the running configuration
- "net.ipv4.conf.all.rp_filter" is correctly set to "1"
  in "/etc/sysctl.conf"
- "net.ipv4.conf.default.rp_filter" is correctly set to "1"
  in the running configuration
- "net.ipv4.conf.default.rp_filter" is correctly set to "1"
  in "/etc/sysctl.conf"
```

3.3.8 Ensure source routed packets are not accepted

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.

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 file in `/etc/sysctl.d/` ending in `conf` :

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

Example:

```
# printf '%s ' "net.ipv4.conf.all.accept_source_route = 0" "net.ipv4.conf.default.accept_source_route = 0" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

- IF - IPv6 is enabled on the system:

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

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

Example:

```
# printf '%s ' "net.ipv6.conf.all.accept_source_route = 0" "net.ipv6.conf.default.accept_source_route = 0" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

```
{ sysctl -w net.ipv6.conf.all.accept_source_route=0 sysctl -w net.ipv6.conf.default.accept_source_route=0  
sysctl -w net.ipv6.route.flush=1 }
```

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\\s]***[\\s]*pass:[\\s]***\$

Hosts

The command script with multiple lines returned :

```
sysctl: cannot stat /proc/sys/net/ipv6/conf/all/disable_ipv6: No such file or directory
```

- Audit Result:

** PASS **

- "net.ipv4.conf.all.accept_source_route" is correctly set to "0"
 in the running configuration
- "net.ipv4.conf.all.accept_source_route" is correctly set to "0"
 in "/etc/sysctl.conf"
- "net.ipv4.conf.default.accept_source_route" is correctly set to "0"
 in the running configuration
- "net.ipv4.conf.default.accept_source_route" is correctly set to "0"
 in "/etc/sysctl.conf"
- IPv6 is disabled on the system, "net.ipv6.conf.all.accept_source_route" is not applicable
- IPv6 is disabled on the system, "net.ipv6.conf.default.accept_source_route" is not applicable

3.3.9 Ensure suspicious packets are logged

Info

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

Setting `net.ipv4.conf.all.log_martians` and `net.ipv4.conf.default.log_martians` to 1 enables this feature. Logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Solution

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

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

Example:

```
# printf '%s ' "net.ipv4.conf.all.log_martians = 1" "net.ipv4.conf.default.log_martians = 1" >> /etc/sysctl.d/60-netip4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.02a.
800-171R3	03.03.02b.
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-3
800-53	AU-3(1)
800-53	AU-7
800-53	AU-12
800-53R5	AU-3

800-53R5	AU-3(1)
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.2.3(c)
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSCV8	8.5
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
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	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***[s]*pass:[s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
  - "net.ipv4.conf.all.log_martians" is correctly set to "1"
    in the running configuration
  - "net.ipv4.conf.all.log_martians" is correctly set to "1"
    in "/etc/ufw/sysctl.conf"
  - "net.ipv4.conf.default.log_martians" is correctly set to "1"
    in the running configuration
  - "net.ipv4.conf.default.log_martians" is correctly set to "1"
    in "/etc/ufw/sysctl.conf"
```

3.3.10 Ensure tcp syn cookies is enabled

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.

Attackers use SYN flood attacks to perform a denial of service attacked on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. Setting `net.ipv4.tcp_syncookies` to 1 enables SYN cookies, allowing the system to keep accepting valid connections, even if under a denial of service attack.

Solution

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

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

Example:

```
# printf '%s ' "net.ipv4.tcp_syncookies = 1" >> /etc/sysctl.d/60-netip4_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6

800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s]***\s]*pass:?\s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- "net.ipv4.tcp_syncookies" is correctly set to "1"
  in the running configuration
- "net.ipv4.tcp_syncookies" is correctly set to "1"
  in "/etc/sysctl.conf"
```

3.3.11 Ensure ipv6 router advertisements are not accepted

Info

Routers periodically multicast Router Advertisement messages to announce their availability and convey information to neighboring nodes that enable them to be automatically configured on the network.

`net.ipv6.conf.all.accept_ra` and `net.ipv6.conf.default.accept_ra` determine the systems ability to accept these advertisements

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes. Setting `net.ipv6.conf.all.accept_ra` and `net.ipv6.conf.default.accept_ra` to 0 disables the system's ability to accept IPv6 router advertisements.

Solution

- IF - IPv6 is enabled on the system:

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

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

Example:

```
# printf '%s ' "net.ipv6.conf.all.accept_ra = 0" "net.ipv6.conf.default.accept_ra = 0" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following script to set the active kernel parameters:

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

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

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6

800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s***\s**pass:?\s***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

sysctl: cannot stat /proc/sys/net/ipv6/conf/all/disable_ipv6: No such file or directory

- Audit Result:

** PASS **

- IPv6 is disabled on the system, "net.ipv6.conf.all.accept_ra" is not applicable
- IPv6 is disabled on the system, "net.ipv6.conf.default.accept_ra" is not applicable

4.1.1 Ensure a single firewall configuration utility is in use

Info

In Linux security, employing a single, effective firewall configuration utility ensures that only legitimate traffic gets processed, reducing the system's exposure to potential threats. The choice between `ufw` `nftables` and `iptables` depends on organizational needs.

Note: `iptables` is being phased out, and support for `iptables` will be reduced over time. It is recommended to transition towards either `nftables` or `ufw` as the default firewall management tool.

Proper configuration of a single firewall utility minimizes cyber threats and protects services and data, while avoiding vulnerabilities like open ports or exposed services. Standardizing on a single tool simplifies management, reduces errors, and fortifies security across Linux systems.

Solution

Remediating to a single firewall configuration is a complex process and involves several steps. The following provides the basic steps to follow for a single firewall configuration:

-

Determine which firewall utility best fits organizational needs

-

Follow the recommendations in the subsequent subsection for the single firewall to be used

Note: Review the firewall subsection overview for the selected firewall to be used, it contains a script to simplify this process.

-

Return to this recommendation to ensure a single firewall configuration utility is in use

Impact:

The use of more than one firewall utility may produce unexpected results.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7

800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1

QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s***\s**pass:?\s***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

Audit Results:

** PASS **

- A single firewall is in use follow the recommendation in ufw subsection ONLY

4.2.1 Ensure ufw is installed

Info

The Uncomplicated Firewall (ufw) is a frontend for iptables and is particularly well-suited for host-based firewalls. ufw provides a framework for managing netfilter, as well as a command-line interface for manipulating the firewall

A firewall utility is required to configure the Linux kernel's netfilter framework via the iptables or nftables back-end.

The Linux kernel's netfilter framework host-based firewall can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

Note: Only one firewall utility should be installed and configured. UFW is dependent on the iptables package

Solution

Run the following command to install Uncomplicated Firewall (UFW):

```
# apt install ufw
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3

CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: `/bin/dpkg -s ufw 2>&1 | /bin/grep -E '(Status:|not installed)'`

expect: `^Status: install ok`

Hosts

192.168.40.171

```
The command '/bin/dpkg -s ufw 2>&1 | /bin/grep -E '(Status:|not installed)'' returned :  
Status: install ok installed
```

4.2.2 Ensure iptables-persistent is not installed with ufw

Info

The iptables-persistent is a boot-time loader for netfilter rules, iptables plugin

Running both ufw and the services included in the iptables-persistent package may lead to conflict

Solution

Run the following command to remove the iptables-persistent package:

```
# apt purge iptables-persistent
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02

CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s iptables-persistent 2>&1 | /bin/grep -E '(^Status:|not installed)'
 expect: (^Status: deinstall ok|not installed)

Hosts

4.2.2 Ensure iptables-persistent is not installed with ufw

192.168.40.171

```
The command '/bin/dpkg -s iptables-persistent 2>&1 | /bin/grep -E '^(Status:|not installed)''  
returned :
```

```
dpkg-query: package 'iptables-persistent' is not installed and no information is available
```

4.2.3 Ensure ufw service is enabled

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.

Note:

- When running ufw enable or starting ufw via its initscript, ufw will flush its chains. This is required so ufw can maintain a consistent state, but it may drop existing connections (eg ssh). ufw does support adding rules before enabling the firewall.

- Run the following command before running ufw enable

```
# ufw allow proto tcp from any to any port 22
```

- The rules will still be flushed, but the ssh port will be open after enabling the firewall. Please note that once ufw is 'enabled', ufw will not flush the chains when adding or removing rules (but will when modifying a rule or changing the default policy)

- By default, ufw will prompt when enabling the firewall while running under ssh. This can be disabled by using ufw --force enable

The ufw service must be enabled and running in order for ufw to protect the system

Solution

Run the following command to unmask the ufw daemon:

```
# systemctl unmask ufw.service
```

Run the following command to enable and start the ufw daemon:

```
# systemctl --now enable ufw.service
```

active

Run the following command to enable ufw:

```
# ufw enable
```

Impact:

Changing firewall settings while connected over network can result in being locked out of the system.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6

800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - check if ufw is enabled

The command '/bin/systemctl is-enabled ufw' returned :

enabled

PASSED - check if ufw is active

The command '/bin/systemctl is-active ufw' returned :

active

PASSED - ufw status active check

The command '/sbin/ufw status | /bin/grep 'Status: active'' returned :

Status: active

4.2.6 Ensure ufw firewall rules exist for all open ports

Info

Services and ports can be accepted or explicitly rejected.

Note:

- Changing firewall settings while connected over network can result in being locked out of the system
- The remediation command opens up the port to traffic from all sources. Consult ufw documentation and set any restrictions in compliance with site policy

To reduce the attack surface of a system, all services and ports should be blocked unless required.

- Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.
- Without a firewall rule configured for open ports, the default firewall policy will drop all packets to these ports.
- Required ports should have a firewall rule created to allow approved connections in accordance with local site policy.
- Unapproved ports should have an explicit deny rule created.

Solution

For each port identified in the audit which does not have a firewall rule, evaluate the service listening on the port and add a rule for accepting or denying inbound connections in accordance with local site policy:

Examples:

```
# ufw allow in <port>/<tcp or udp protocol>
```

```
# ufw deny in <port>/<tcp or udp protocol>
```

Note: Examples create rules for from any, to any. More specific rules should be concentrated when allowing inbound traffic e.g only traffic from this network.

Example to allow traffic on port 443 using the tcp protocol from the 192.168.1.0 network:

```
ufw allow from 192.168.1.0/24 to any proto tcp port 443
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06

800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1

PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^none\$

Hosts

192.168.40.171

```
The command script with multiple lines returned :
none
```

4.3.1 Ensure nftables is installed

Info

nftables provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM) and a new nft userspace command line tool. nftables reuses the existing Netfilter subsystems such as the existing hook infrastructure, the connection tracking system, NAT, userspace queuing and logging subsystem.

Notes:

- nftables is available in Linux kernel 3.13 and newer
- Only one firewall utility should be installed and configured
- Changing firewall settings while connected over the network can result in being locked out of the system

nftables is a subsystem of the Linux kernel that can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

Solution

Run the following command to install nftables :

```
# apt install nftables
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4

CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.3.2 Ensure ufw is uninstalled or disabled with nftables

Info

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed to be easy to use. Running both the nftables service and ufw may lead to conflict and unexpected results.

NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

Solution

Run one of the following to either remove ufw or disable ufw and mask ufw.service :

Run the following command to remove ufw :

```
# apt purge ufw  
  
-OR-
```

Run the following commands to disable ufw and mask ufw.service :

```
# ufw disable # systemctl stop ufw.service # systemctl mask ufw.service
```

Note: ufw disable needs to be run before systemctl mask ufw.service in order to correctly disable UFW

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5

CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.3.3 Ensure iptables are flushed with nftables

Info

nftables is a replacement for iptables, ip6tables, ebtables and arptables

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: The identified firewall 'nftables' was not found to be active and this check does not apply.

Solution

Run the following commands to flush iptables:

For iptables:

```
# iptables -F
```

For ip6tables:

```
# ip6tables -F
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5

CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1M
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.3.4 Ensure a nftables 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.

nftables doesn't have any default tables. Without a table being built, nftables will not filter network traffic.

NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

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/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1

CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.3.5 Ensure nftables base chains exist

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.

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.

NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

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/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7

800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2

QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.3.6 Ensure nftables loopback traffic is configured

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network

Loopback traffic is generated between processes on machine and is typically critical to the 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.

NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

Solution

Run the following commands to implement the loopback rules:

```
# nft add rule inet filter input iif lo accept # nft add 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/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1

CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.3.7 Ensure nftables outbound and established connections are configured

Info

Configure the firewall rules for new outbound, and established connections

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: The identified firewall 'nftables' was not found to be active and this check does not apply.

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 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
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3

CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1M
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.3.8 Ensure nftables default deny firewall policy

Info

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

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 allow list acceptable usage than to deny list unacceptable usage.

Note:

- Allow port 22(ssh) needs to be updated to only allow systems requiring ssh connectivity to connect, as per site policy.
- Changing firewall settings while connected over network can result in being locked out of the system.

NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06

800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.3.9 Ensure nftables service is enabled

Info

The nftables service allows for the loading of nftables rulesets during boot, or starting on the nftables service

The nftables service restores the nftables rules from the rules files referenced in the /etc/nftables.conf file during boot or the starting of the nftables service

NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

Solution

Run the following command to enable the nftables service:

```
# systemctl enable nftables
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01

CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.3.10 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.

Note: Saving the script and following the instruction in the Configure nftables section overview will implement the rules in the configure nftable section, open port 22(ssh) from anywhere, and applies nftables ruleset on boot.

Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot

NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

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/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7

800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2

QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.4.1.1 Ensure iptables packages are installed

Info

iptables is a utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall, implemented as different Netfilter modules, and the chains and rules it stores. Different kernel modules and programs are used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.

A method of configuring and maintaining firewall rules is necessary to configure a Host Based Firewall.

NOTE: The identified firewall 'iptables' was not found to be active and this check does not apply.

Solution

Run the following command to install iptables and iptables-persistent

```
# apt install iptables iptables-persistent
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4

CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.4.1.2 Ensure nftables is not in use with iptables

Info

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables.

Running both iptables and nftables may lead to conflict.

NOTE: The identified firewall 'iptables' was not found to be active and this check does not apply.

Solution

Run the following command to remove nftables :

```
# apt purge nftables
```

- OR -

Run the following commands to stop and mask nftables.service :

```
# systemctl stop nftables.service # systemctl mask nftables.service
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5

CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.4.1.3 Ensure ufw is not in use with iptables

Info

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed to be easy to use.

- Uses a command-line interface consisting of a small number of simple commands
- Uses iptables for configuration

Running iptables.persistent with ufw enabled may lead to conflict and unexpected results.

NOTE: The identified firewall 'iptables' was not found to be active and this check does not apply.

Solution

Run the following command to remove ufw :

```
# apt purge ufw
```

- OR -

Run the following commands to disable ufw, and stop and mask ufw.service :

```
# ufw disable # systemctl stop ufw.service # systemctl mask ufw.service
```

Note: ufw disable needs to be run before systemctl mask ufw.service in order to correctly disable UFW

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4

CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.4.2.1 Ensure iptables default deny firewall policy

Info

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

Notes:

- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well

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

NOTE: The identified firewall 'iptables' was not found to be active and this check does not apply.

Solution

Run the following commands to implement a default DROP policy:

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1
CSF	ID.AM-3

CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.4.2.2 Ensure iptables loopback traffic is configured

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).

Note:

- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well

Loopback traffic is generated between processes on machine and is typically critical to the operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

NOTE: The identified firewall 'iptables' was not found to be active and this check does not apply.

Solution

Run the following commands to implement the loopback rules:

```
# iptables -A INPUT -i lo -j ACCEPT # iptables -A OUTPUT -o lo -j ACCEPT # iptables -A INPUT -s 127.0.0.0/8 -j DROP
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5

CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.4.2.3 Ensure iptables outbound and established connections are configured

Info

Configure the firewall rules for new outbound, and established connections.

Note:

- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well

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: The identified firewall 'iptables' was not found to be active and this check does not apply.

Solution

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT # iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT # iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT # iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5

CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1M
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.4.2.4 Ensure iptables firewall rules exist for all open ports

Info

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

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

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

NOTE: The identified firewall 'iptables' was not found to be active and this check does not apply.

Solution

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5

CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.4.3.1 Ensure iptables default deny firewall policy

Info

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

Note:

- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well

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

NOTE: The identified firewall 'iptables' was not found to be active and this check does not apply.

Solution

- IF - IPv6 is enabled on your system:

Run the following commands to implement a default DROP policy:

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1

CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

Policy Value

PASSED

Hosts

192.168.40.171

4.4.3.2 Ensure iptables loopback traffic is configured

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1).

Note:

- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well

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.

NOTE: The identified firewall 'iptables' was not found to be active and this check does not apply.

Solution

Run the following commands to implement the loopback rules:

```
# iptables -A INPUT -i lo -j ACCEPT # iptables -A OUTPUT -o lo -j ACCEPT # iptables -A INPUT -s ::1 -j DROP
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5

CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.4.3.3 Ensure iptables outbound and established connections are configured

Info

Configure the firewall rules for new outbound, and established IPv6 connections.

Note:

- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well

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: The identified firewall 'iptables' was not found to be active and this check does not apply.

Solution

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT # iptables -A OUTPUT -p udp  
-m state --state NEW,ESTABLISHED -j ACCEPT # iptables -A INPUT -p tcp -m state --state ESTABLISHED -j  
ACCEPT # iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5

CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1M
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

4.4.3.4 Ensure iptables firewall rules exist for all open ports

Info

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

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

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

NOTE: The identified firewall 'iptables' was not found to be active and this check does not apply.

Solution

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5

CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1A
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

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

Info

The file /etc/ssh/sshd_config and files ending inconf in the /etc/ssh/sshd_config.d directory, contain configuration specifications for sshd

configuration specifications for sshd need to be protected from unauthorized changes by non-privileged users.

Solution

Run the following script to set ownership and permissions on /etc/ssh/sshd_config and files ending inconf in the /etc/ssh/sshd_config.d directory:

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

{ chmod u-x,og-rwx /etc/ssh/sshd_config chown root:root /etc/ssh/sshd_config while IFS= read -r -d '$0'
l_file; do if [ -e "$l_file" ]; then chmod u-x,og-rwx "$l_file"
chown root:root "$l_file"
fi done < <(find /etc/ssh/sshd_config.d -type f -print0 2>/dev/null) }

- IF - other locations are listed in an Include statement, *.conf files in these locations access should also be modified.
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5

800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2

NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***\[s]*pass:?\[s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

- Audit Result:
*** PASS ***

```
- * Correctly set * :  
- File: "/etc/ssh/sshd_config":  
  - Correct: mode (0600), owner (root), and group owner (root) configured
```

5.1.2 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.

If an unauthorized user obtains the private SSH host key file, the host could be impersonated

Solution

Run the following script to set mode, ownership, and group on the private SSH host key files:

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

```
{ a_output=(); a_output2=(); l_ssh_group_name="$(awk -F: '($1 ~ /^(ssh_keys|_?ssh)$/) {print $1}' /etc/group)"
f_file_access_fix() { while IFS=: read -r l_file_mode l_file_owner l_file_group; do a_out2=() [ "$l_file_group" =
"$l_ssh_group_name" ] && l_pmask="0137" || l_pmask="0177"
l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
if [ $(( $l_file_mode & $l_pmask )) -gt 0 ]; then a_out2+=(" Mode: \"$l_file_mode\" should be mode:
\"$l_maxperm\" or more restrictive" " updating to mode: :$l_maxperm\"") if [ "$l_file_group" =
"$l_ssh_group_name" ]; then chmod u-x,g-wx,o-rwx "$l_file"
else chmod u-x,go-rwx "$l_file"
fi fi if [ "$l_file_owner" != "root" ]; then a_out2+=(" Owned by: \"$l_file_owner\" should be owned by \"root\"""
" Changing ownership to \"root\"") chown root "$l_file"
fi if [ ! "$l_file_group" =~ ($l_ssh_group_name|root) ]; then [ -n "$l_ssh_group_name" ] &&
l_new_group="$l_ssh_group_name" || l_new_group="root"
a_out2+=(" Owned by group \"$l_file_group\" should be group owned by: \"$l_ssh_group_name\" or \"root
\""" " Changing group ownership to \"$l_new_group\"") chgrp "$l_new_group" "$l_file"
fi if [ "${#a_out2[@]}" -gt "0" ]; then a_output2+=(" - File: \"$l_file\" "" "${a_out2[@]}") else a_output+=(" - File:
\"$l_file\" "" "Correct: mode: \"$l_file_mode\", owner: \"$l_file_owner\", and group owner: \"$l_file_group
\" configured") fi done < <(stat -Lc '%a:%U:%G' "$l_file") } while IFS= read -r -d $'0' l_file; do if ssh-
keygen -lf &>/dev/null "$l_file"; then file "$l_file" | grep -Piq -- 'bopensshh+([^# r]+h+)?privateh+keyb' &&
f_file_access_fix fi done < <(find -L /etc/ssh -xdev -type f -print0 2>/dev/null) if [ "${#a_output2[@]}" -le "0" ];
then printf '%s' ' "" " - No access changes required" ""
else printf '%s' ' "" " - Remediation results:" "${a_output2[@]}" ""
fi }
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171

3.1.1

800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7

ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s***\s**pass:?\s***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
  - File: "/etc/ssh/ssh_host_dsa_key"
    Correct: mode: "0600", owner: "root" and group owner: "root" configured
  - File: "/etc/ssh/ssh_host_rsa_key"
    Correct: mode: "0600", owner: "root" and group owner: "root" configured
  - File: "/etc/ssh/ssh_host_ed25519_key"
    Correct: mode: "0600", owner: "root" and group owner: "root" configured
  - File: "/etc/ssh/ssh_host_ecdsa_key"
    Correct: mode: "0600", owner: "root" and group owner: "root" configured
```

5.1.3 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.

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Solution

Run the following script to set mode, ownership, and group on the public SSH host key files:

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

```
{ a_output=(); a_output2=() I_pmask="0133"; I_maxperm="$( printf '%o' $(( 0777 & ~I_pmask )) )"
f_file_access_fix() { while IFS=: read -r I_file_mode I_file_owner I_file_group; do a_out2=() [ $(( I_file_mode
& I_pmask )) -gt 0 ] && a_out2+=(" Mode: \"$I_file_mode\" should be mode: \"$I_maxperm\" or more
restrictive" " updating to mode: \"$I_maxperm\"") && chmod u-x,go-wx "$I_file"
[ "$I_file_owner" != "root" ] && a_out2+=(" Owned by: \"$I_file_owner\" should be owned by \"root\" "
Changing ownership to \"root\"") && chown root "$I_file"
[ "$I_file_group" != "root" ] && a_out2+=(" Owned by group \"$I_file_group\" should be group owned by:
\"root\" " Changing group ownership to \"root\"") && chgrp root "$I_file"
if [ "${#a_out2[@]}" -gt "0" ]; then a_output2+=(" - File: \"$I_file\" \"${a_out2[@]}") else a_output+=(" - File:
 \"$I_file\" \" Correct: mode: \"$I_file_mode\", owner: \"$I_file_owner\", and group owner: \"$I_file_group
 \" configured") fi done < <(stat -Lc '%a:%U:%G' "$I_file") } while IFS= read -r -d $'0' I_file; do if ssh-
keygen -lf &>/dev/null "$I_file"; then file "$I_file" | grep -Piq -- 'bopenssh+([^\# r]+h+)?public+keyb' &&
f_file_access_fix fi done < <(find -L /etc/ssh -xdev -type f -print0 2>/dev/null) if [ "${#a_output2[@]}" -le "0" ];
then printf '%s ' "" " - No access changes required" ""
else printf '%s ' " - Remediation results:" "${a_output2[@]}" ""
fi }
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04

800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1

ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?:i)^\s***\s*\s*pass:?\s***\s*\$

Hosts

192.168.40.171

The command script with multiple lines returned :

- Audit Result:

** PASS **

- File: "/etc/ssh/ssh_host_rsa_key.pub"

Correct: mode: "0644", owner: "root" and group owner: "root" configured

- File: "/etc/ssh/ssh_host_dsa_key.pub"

Correct: mode: "0644", owner: "root" and group owner: "root" configured

- File: "/etc/ssh/ssh_host_ecdsa_key.pub"

Correct: mode: "0644", owner: "root" and group owner: "root" configured

- File: "/etc/ssh/ssh_host_ed25519_key.pub"

Correct: mode: "0644", owner: "root" and group owner: "root" configured

5.1.4 Ensure sshd access is configured

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.

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 parameters above any Include and Match set statements as follows:

AllowUsers <userlist>

- AND/OR - AllowGroups <grouplist>

Note:

- First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in aconf file in a Include directory.

- Be advised that these options are "ANDed" together. If both AllowUsers and AllowGroups are set, connections will be limited to the list of users that are also a member of an allowed group. It is recommended that only one be set for clarity and ease of administration.

- It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user or group and forget to add it to the deny list.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	4.3
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2

QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
port 22: allowusers nallen
allowusers mf_dev
allowusers c4197
allowusers cms
allowusers root
allowusers c4290
allowusers c3311
allowusers c3640
allowusers c4363
Pass
```

5.1.7 Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured

Info

Note: To clarify, the two settings described below are only meant for idle connections from a protocol perspective and are not meant to check if the user is active or not. An idle user does not mean an idle connection. SSH does not and never had, intentionally, the capability to drop idle users. In SSH versions before 8.2p1 there was a bug that caused these values to behave in such a manner that they were abused to disconnect idle users. This bug has been resolved in 8.2p1 and thus it can no longer be abused to disconnect idle users.

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of SSH sessions. Taken directly from `man 5 sshd_config` :

-

`ClientAliveInterval` Sets a timeout interval in seconds after which if no data has been received from the client, `sshd(8)` will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client.

-

`ClientAliveCountMax` Sets the number of client alive messages which may be sent without `sshd(8)` receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, `sshd` will disconnect the client, terminating the session. It is important to note that the use of client alive messages is very different from `TCPKeepAlive`. The client alive messages are sent through the encrypted channel and therefore will not be spoofable. The `TCP keepalive` option enabled by `TCPKeepAlive` is spoofable. The client alive mechanism is valuable when the client or server depend on knowing when a connection has become unresponsive. The default value is 3. If `ClientAliveInterval` is set to 15, and `ClientAliveCountMax` is left at the default, unresponsive SSH clients will be disconnected after approximately 45 seconds. Setting a zero `ClientAliveCountMax` disables connection termination.

In order to prevent resource exhaustion, appropriate values should be set for both `ClientAliveInterval` and `ClientAliveCountMax`. Specifically, looking at the source code, `ClientAliveCountMax` must be greater than zero in order to utilize the ability of SSH to drop idle connections. If connections are allowed to stay open indefinitely, this can potentially be used as a DDOS attack or simple resource exhaustion could occur over unreliable networks.

The example set here is a 45 second timeout. Consult your site policy for network timeouts and apply as appropriate.

Solution

Edit the `/etc/ssh/sshd_config` file to set the `ClientAliveInterval` and `ClientAliveCountMax` parameters above any `Include` and `Match` entries according to site policy.

Example:

```
ClientAliveInterval 15 ClientAliveCountMax 3
```

Note: First occurrence of a option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.11
800-171R3	03.01.11
800-53	AC-12
800-53R5	AC-12
CN-L3	7.1.2.2(d)
CN-L3	7.1.3.7(b)
CN-L3	8.1.4.1(b)
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ITSG-33	AC-12
LEVEL	1A
NIAV2	NS49

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - ClientAliveCountMax is greater than 0
The command script with multiple lines returned :

port 22: clientalivecountmax 3
Pass

PASSED - ClientAliveInterval is greater than 0
The command script with multiple lines returned :

port 22: clientaliveinterval 15
Pass

5.1.10 Ensure sshd HostbasedAuthentication is disabled

Info

The HostbasedAuthentication parameter specifies if authentication is allowed through trusted hosts via the user ofrhosts or /etc/hosts.equiv along with successful public key client host authentication.

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

Solution

Edit the /etc/ssh/sshd_config file to set the HostbasedAuthentication parameter to no above any Include and Match entries as follows:

HostbasedAuthentication no

Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06b.
800-53	CM-7b.
800-53R5	CM-7b.
CN-L3	7.1.3.5(c)
CN-L3	7.1.3.7(d)
CN-L3	8.1.4.4(b)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
LEVEL	1A
NIAV2	SS13b
NIAV2	SS14a
NIAV2	SS14c
PCI-DSSV3.2.1	2.2.2
PCI-DSSV4.0	2.2.4

QCSC-V1	3.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
port 22: hostbasedauthentication no
Pass
```

5.1.11 Ensure sshd IgnoreRhosts is enabled

Info

The IgnoreRhosts parameter specifies that rhosts and shosts files will not be used in RhostsRSAAuthentication or HostbasedAuthentication

Setting this parameter forces users to enter a password when authenticating with SSH.

Solution

Edit the /etc/ssh/sshd_config file to set the IgnoreRhosts parameter to yes above any Include and Match entries as follows:

IgnoreRhosts yes

Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

```
The command script with multiple lines returned :
```

```
port 22: ignorerhosts yes  
Pass
```

5.1.12 Ensure sshd KexAlgorithms is configured

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

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 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

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

Solution

Edit the `/etc/ssh/sshd_config` file and add/modify the `KexAlgorithms` line to contain a comma separated list of the site unapproved (weak) `KexAlgorithms` preceded with a `-` above any `Include` entries:

Example:

`KexAlgorithms -diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1`

Note: First occurrence of an option takes precedence. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8

800-171R3	03.05.07
800-171R3	03.05.12
800-171R3	03.13.08
800-53	AC-17(2)
800-53	IA-5
800-53	IA-5(1)
800-53	SC-8
800-53	SC-8(1)
800-53R5	AC-17(2)
800-53R5	IA-5
800-53R5	IA-5(1)
800-53R5	SC-8
800-53R5	SC-8(1)
CN-L3	7.1.2.7(g)
CN-L3	7.1.3.1(d)
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.1(c)
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
CSCV8	3.10
CSF	PR.AC-1
CSF	PR.AC-3
CSF	PR.DS-2
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
CSF2.0	PR.AA-05
CSF2.0	PR.DS-02
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10

ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO-27001-2022	A.5.33
ISO-27001-2022	A.6.7
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.2.2
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	AC-17(2)
ITSG-33	IA-5
ITSG-33	IA-5(1)
ITSG-33	SC-8
ITSG-33	SC-8a.
ITSG-33	SC-8(1)
LEVEL	1A
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T5.2.3
NESA	T5.4.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	AM37
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS5d
NIAV2	NS6b
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	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	2.1
SWIFT-CSCV1	2.6

SWIFT-CSCV1	4.1
TBA-FIISB	29.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
port 22: kexalgorithms sntrup761x25519-sha512@openssh.com,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
Pass
```


5.1.13 Ensure sshd LoginGraceTime is configured

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.

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 LoginGraceTime parameter to 60 seconds or less above any Include entry as follows:

LoginGraceTime 60

Note: First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.11
800-171R3	03.01.11
800-53	AC-10
800-53	AC-12
800-53R5	AC-10
800-53R5	AC-12
CN-L3	7.1.2.2(d)
CN-L3	7.1.3.7(b)
CN-L3	8.1.4.1(b)
CSF2.0	PR.AA-03
CSF2.0	PR.AA-05
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ITSG-33	AC-10
ITSG-33	AC-12
LEVEL	1A
NESA	T5.5.1

NIAV2	NS49
QCSC-V1	5.2.1
QCSC-V1	5.2.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
port 22: loginracetime 60
Pass
```

5.1.14 Ensure sshd LogLevel is configured

Info

SSH provides several logging levels with varying amounts of verbosity. The DEBUG options are specifically not recommended other than strictly for debugging SSH communications. These levels provide so much data that it is difficult to identify important security information, and may violate the privacy of users.

The 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.

The 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.

Solution

Edit the `/etc/ssh/sshd_config` file to set the LogLevel parameter to VERBOSE or INFO above any Include and Match entries as follows:

LogLevel VERBOSE
- OR - LogLevel INFO

Note: First occurrence of an option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)

CSCV7	6.2
CSCV7	6.3
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
port 22: loglevel VERBOSE
Pass
```

5.1.15 Ensure sshd MACs are configured

Info

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

Notes:

- Some organizations may have stricter requirements for approved MACs.
- Ensure that MACs used are in compliance with site policy.
- The only "strong" MACs currently FIPS 140 approved are:
 - HMAC-SHA1
 - HMAC-SHA2-256
 - HMAC-SHA2-384
 - HMAC-SHA2-512

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.

Solution

Edit the `/etc/ssh/sshd_config` file and add/modify the MACs line to contain a comma separated list of the site unapproved (weak) MACs preceded with a - above any Include entries:

Example:

MACs -hmac-md5,hmac-md5-96,hmac-ripemd160,hmac-sha1-96,umac-64@openssh.com,hmac-md5-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com

- IF - CVE-2023-48795 has not been reviewed and addressed, the following etm MACs should be added to the exclude list:

hmac-sha1-etm@openssh.com

,

hmac-sha2-256-etm@openssh.com

,

hmac-sha2-512-etm@openssh.com

Note: First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
800-171R3	03.05.07
800-171R3	03.05.12
800-171R3	03.13.08
800-53	AC-17(2)
800-53	IA-5
800-53	IA-5(1)
800-53	SC-8
800-53	SC-8(1)
800-53R5	AC-17(2)
800-53R5	IA-5
800-53R5	IA-5(1)
800-53R5	SC-8
800-53R5	SC-8(1)
CN-L3	7.1.2.7(g)
CN-L3	7.1.3.1(d)
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.1(c)
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
CSCV8	3.10
CSF	PR.AC-1
CSF	PR.AC-3
CSF	PR.DS-2
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
CSF2.0	PR.AA-05
CSF2.0	PR.DS-02
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO-27001-2022	A.5.33
ISO-27001-2022	A.6.7
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.2.2
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	AC-17(2)
ITSG-33	IA-5
ITSG-33	IA-5(1)
ITSG-33	SC-8
ITSG-33	SC-8a.
ITSG-33	SC-8(1)
LEVEL	1A
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T5.2.3
NESA	T5.4.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	AM37
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS5d
NIAV2	NS6b
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	3.2
QCSC-V1	5.2.1

QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	2.1
SWIFT-CSCV1	2.6
SWIFT-CSCV1	4.1
TBA-FIISB	29.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
port 22: macs umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
Pass
```

5.1.16 Ensure sshd MaxAuthTries is configured

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.

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 MaxAuthTries parameter to 4 or less above any Include and Match entries as follows:

MaxAuthTries 4

Note: First occurrence of an option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.02a.
800-171R3	03.03.02b.
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-3
800-53	AU-3(1)
800-53	AU-7
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-3(1)
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.2.3(c)
CN-L3	7.1.3.3(a)

CN-L3	7.1.3.3(b)
CN-L3	8.1.4.3(b)
CSCV7	16.13
CSCV8	8.5
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
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	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
port 22: maxauthtries 4
Pass
```

5.1.17 Ensure sshd MaxSessions is configured

Info

The MaxSessions parameter specifies the maximum number of open sessions permitted from a given connection.

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 MaxSessions parameter to 10 or less above any Include and Match entries as follows:

MaxSessions 10

Note: First occurrence of an option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-53	AC-10
800-53R5	AC-10
CSF2.0	PR.AA-05
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	AC-10
LEVEL	1A
NESA	T5.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - config file MaxSessions setting

Compliant file(s):

/etc/ssh/sshd_config - regex '^[\\s]*(?i)MaxSessions(?-i)[\\s] ' found - expect '^[\\s]*(?i)MaxSessions(?-i)[\\s]+"(1[1-9]|[2-9][0-9]|[1-9][0-9][0-9]+)"?[\\s]*\$' not found in the following lines:

38: MaxSessions 10

/etc/ssh/sshd_config.d/50-cloud-init.conf - regex not found

PASSED - sshd maxsessions setting

The command script with multiple lines returned :

port 22: maxsessions 10

Pass

5.1.18 Ensure sshd MaxStartups is configured

Info

The MaxStartups parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.

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 MaxStartups parameter to 10:30:60 or more restrictive above any Include entries as follows:

MaxStartups 10:30:60

Note: First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-53	AC-10
800-53R5	AC-10
CSF2.0	PR.AA-05
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	AC-10
LEVEL	1A
NESA	T5.5.1
QCSC-V1	5.2.1
QCSC-V1	5.2.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
port 22: maxstartups 10:30:60
Pass
```


5.1.19 Ensure sshd PermitEmptyPasswords is disabled

Info

The PermitEmptyPasswords parameter specifies if the SSH server allows login to accounts with empty password strings.

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system.

Solution

Edit /etc/ssh/sshd_config and set the PermitEmptyPasswords parameter to no above any Include and Match entries as follows:

```
PermitEmptyPasswords no
```

Note: First occurrence of an option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

```
The command script with multiple lines returned :
```

```
port 22: permitemptypasswords no  
Pass
```

5.1.21 Ensure sshd PermitUserEnvironment is disabled

Info

The PermitUserEnvironment option allows users to present environment options to the SSH daemon.

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 PermitUserEnvironment parameter to no above any Include entries as follows:

PermitUserEnvironment no

Note: First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06b.
800-53	CM-7b.
800-53R5	CM-7b.
CN-L3	7.1.3.5(c)
CN-L3	7.1.3.7(d)
CN-L3	8.1.4.4(b)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
LEVEL	1A
NIAV2	SS13b
NIAV2	SS14a
NIAV2	SS14c
PCI-DSSV3.2.1	2.2.2
PCI-DSSV4.0	2.2.4
QCSC-V1	3.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

```
The command script with multiple lines returned :
```

```
port 22: permituserenvironment no  
Pass
```

5.1.22 Ensure sshd UsePAM is enabled

Info

The UsePAM directive enables the Pluggable Authentication Module (PAM) interface. If set to yes this will enable PAM authentication using ChallengeResponseAuthentication and PasswordAuthentication directives in addition to PAM account and session module processing for all authentication types.

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 UsePAM parameter to yes above any Include entries as follows:

UsePAM yes

Note: First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass\$

Hosts

192.168.40.171

```
The command script with multiple lines returned :
```

```
port 22: usepam yes
Pass
```

5.2.1 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.

sudo supports a plug-in architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plug-ins to work seamlessly with the sudo front end. The default security policy is sudoers which is configured via the file /etc/sudoers and any entries in /etc/sudoers.d

The security policy determines what privileges, if any, a user has to run sudo. The policy may require that users authenticate themselves with a password or another authentication mechanism. If authentication is required, sudo will exit if the user's password is not entered within a configurable time limit. This limit is policy-specific.

Solution

First determine if LDAP functionality is required. If so, then install sudo-ldap else install sudo

Example:

```
# apt install sudo
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.5
800-171	3.1.6
800-171R3	03.01.06a.
800-171R3	03.01.06b.
800-53	AC-6(2)
800-53	AC-6(5)
800-53R5	AC-6(2)
800-53R5	AC-6(5)
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSCV7	4.3
CSCV8	5.4
CSF	PR.AC-4
CSF2.0	PR.AA-05

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	1A
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.6.1
NIAV2	AM1
NIAV2	AM23f
NIAV2	AM32
NIAV2	AM33
NIAV2	SS13c
NIAV2	SS15c
NIAV2	VL3a
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
SWIFT-CSCV1	1.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

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

Hosts

192.168.40.171

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: 3464
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Multi-Arch: foreign
Version: 1.9.15p5-3ubuntu5
Replaces: sudo-ldap
Depends: libapparmor1 (>= 2.7.0~beta1+bzr1772), libaudit1 (>= 1:2.2.1), libc6 (>= 2.38), libpam0g
(>= 0.99.7.1), libselinux1 (>= 3.1~), libssl1.3t64 (>= 3.0.0), zlib1g (>= 1:1.2.0.2), libpam-modules
Conflicts: sudo-ldap
Conffiles:
/etc/pam.d/sudo b3a1b916bf62a2cc3280f7f9b94844ff
/etc/pam.d/sudo-i ce9740f66cedf7716e26950abfe556fa
/etc/sudo.conf 8c714b777580faea54a2eb6d5f17ad1d
/etc/sudo_logsrvd.conf ad0ba586da300ae3ba46312ad744a6e2
/etc/sudoers 8c20cd717552790f2312db0981337945
/etc/sudoers.d/README bbleba13940f331e91cfb9294d86a04f
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/
Original-Maintainer: Sudo Maintainers <sudo@packages.debian.org>

Use dpkg --info (= dpkg-deb --info) to examine archive files.

```

5.2.2 Ensure sudo commands use pty

Info

sudo can be configured to run only from a pseudo terminal (pseudo-pty).

Attackers can run a malicious program using sudo which would fork a background process that remains even when the main program has finished executing.

Solution

Edit the file /etc/sudoers with visudo or a file in /etc/sudoers.d/ with visudo -f <PATH TO FILE> and add the following line:

Defaults use_pty

Edit the file /etc/sudoers with visudo and any files in /etc/sudoers.d/ with visudo -f <PATH TO FILE> and remove any occurrence of !use_pty

Note:

- sudo will read each file in /etc/sudoers.d skipping file names that end in ~ or contain a character to avoid causing problems with package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, /etc/sudoers.d/01_first will be parsed before /etc/sudoers.d/10_second
- Be aware that because the sorting is lexical, not numeric, /etc/sudoers.d/1_whoops would be loaded after /etc/sudoers.d/10_second
- Using a consistent number of leading zeroes in the file names can be used to avoid such problems.

Impact:

WARNING: Editing the sudo configuration incorrectly can cause sudo to stop functioning. Always use visudo to modify sudo configuration files.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.5
800-171	3.1.6
800-171R3	03.01.06a.
800-171R3	03.01.06b.
800-53	AC-6(2)
800-53	AC-6(5)
800-53R5	AC-6(2)
800-53R5	AC-6(5)
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSCV7	5.1
CSCV8	5.4
CSF	PR.AC-4
CSF2.0	PR.AA-05
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	1A
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.6.1
NIAV2	AM1
NIAV2	AM23f
NIAV2	AM32
NIAV2	AM33
NIAV2	SS13c
NIAV2	SS15c
NIAV2	VL3a
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
SWIFT-CSCV1	1.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - /etc/sudoers use_pty

The command '/bin/grep -rPi -- '^h*Defaults\h+([^\n\r]+,\h*)?use_pty\b' /etc/sudoers*' returned :

/etc/sudoers:Defaultsuse_pty

/etc/sudoers.d/pkg-dist:Defaultsuse_pty

/etc/sudoers.tmp.save:Defaultsuse_pty

PASSED - /etc/sudoers !use_pty

The command '/bin/grep -rPi -- '^h*Defaults\h+([^\n\r]+,\h*)?!use_pty\b' /etc/sudoers* | /bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}' returned :

pass

5.2.3 Ensure sudo log file exists

Info

sudo can use a custom log file

A sudo log file simplifies auditing of sudo commands

Solution

Edit the file /etc/sudoers or a file in /etc/sudoers.d/ with visudo or visudo -f <PATH TO FILE> and add the following line:

Example:

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

Note:

- sudo will read each file in /etc/sudoers.d skipping file names that end in ~ or contain a character to avoid causing problems with package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, /etc/sudoers.d/01_first will be parsed before /etc/sudoers.d/10_second
- Be aware that because the sorting is lexical, not numeric, /etc/sudoers.d/1_whoops would be loaded after /etc/sudoers.d/10_second
- Using a consistent number of leading zeroes in the file names can be used to avoid such problems.

Impact:

WARNING: Editing the sudo configuration incorrectly can cause sudo to stop functioning. Always use visudo to modify sudo configuration files.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.02a.
800-171R3	03.03.02b.
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-3
800-53	AU-3(1)
800-53	AU-7
800-53	AU-12

800-53R5	AU-3
800-53R5	AU-3(1)
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.2.3(c)
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	8.1.4.3(b)
CSCV7	6.3
CSCV8	8.5
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
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	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: (i)^\h*Defaults\h+([^\#]+\h*)?logfile\h*=\h*(\"|\')?\H+(\"|\')?(,\h*\H+\h*)*\h*(#.*)?\$ file: /etc/sudoers /etc/sudoers.d/* min_occurrences: 1 regex: (i)^\h*Defaults\h+([^\#]+\h*)?logfile\h*=\h*(\"|\')?\H+(\"|\')?(,\h*\H+\h*)*\h*(#.*)?\$ string_required: NO

Hosts

192.168.40.171

```
Compliant file(s):
/etc/sudoers - regex '(i)^\h*Defaults\h+([^\#]+\h*)?logfile\h*=\h*(\"|\')?\H+(\"|\')?(,\h*\H+\h*)*\h*(#.*)?$' found - expect '(i)^\h*Defaults\h+([^\#]+\h*)?logfile\h*=\h*(\"|\')?\H+(\"|\')?(,\h*\H+\h*)*\h*(#.*)?$' found in the following lines:
13: Defaultslogfile="/var/log/sudo.log"
/etc/sudoers.d/README - regex not found
```

5.2.5 Ensure re-authentication for privilege escalation is not disabled globally

Info

The operating system must be configured so that users must re-authenticate for privilege escalation.

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Solution

Configure the operating system to require users to reauthenticate for privilege escalation.

Based on the outcome of the audit procedure, use visudo -f <PATH TO FILE> to edit the relevant sudoers file.

Remove any occurrences of !authenticate tags in the file(s).

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.5
800-171	3.1.6
800-171R3	03.01.06a.
800-171R3	03.01.06b.
800-53	AC-6(2)
800-53	AC-6(5)
800-53R5	AC-6(2)
800-53R5	AC-6(5)
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSCV7	4.3
CSCV8	5.4
CSF	PR.AC-4
CSF2.0	PR.AA-05
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15

ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	1A
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.6.1
NIAV2	AM1
NIAV2	AM23f
NIAV2	AM32
NIAV2	AM33
NIAV2	SS13c
NIAV2	SS15c
NIAV2	VL3a
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
SWIFT-CSCV1	1.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: ^[^\#].*!authenticate file: /etc/sudoers /etc/sudoers.d/* regex: ^[^\#].*!authenticate

Hosts

192.168.40.171

```
The following file(s) do not contain "[^\#].*!authenticate":
/etc/sudoers
/etc/sudoers.d/README
```

5.2.6 Ensure sudo authentication timeout is configured correctly

Info

sudo caches used credentials for a default of 15 minutes. This is for ease of use when there are multiple administrative tasks to perform. The timeout can be modified to suit local security policies.

This default is distribution specific. See audit section for further information.

Setting a timeout value reduces the window of opportunity for unauthorized privileged access to another user.

Solution

If the currently configured timeout is larger than 15 minutes, edit the file listed in the audit section with `visudo -f <PATH TO FILE>` and modify the entry `timestamp_timeout=` to 15 minutes or less as per your site policy. The value is in minutes. This particular entry may appear on it's own, or on the same line as `env_reset` See the following two examples:

Defaults env_reset, timestamp_timeout=15 Defaults timestamp_timeout=15 Defaults env_reset

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.5
800-171	3.1.6
800-171R3	03.01.06a.
800-171R3	03.01.06b.
800-53	AC-6(2)
800-53	AC-6(5)
800-53R5	AC-6(2)
800-53R5	AC-6(5)
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSCV7	4.3
CSCV8	5.4
CSF	PR.AC-4
CSF2.0	PR.AA-05
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15

ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(2)
ITSG-33	AC-6(5)
LEVEL	1A
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.6.1
NIAV2	AM1
NIAV2	AM23f
NIAV2	AM32
NIAV2	AM33
NIAV2	SS13c
NIAV2	SS15c
NIAV2	VL3a
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
SWIFT-CSCV1	1.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

One of the following must pass to satisfy this requirement:

```
-----
PASSED - sudo timeout
The command '/bin/sudo -V | /bin/grep 'Authentication timestamp timeout:'' returned :

Authentication timestamp timeout: 15.0 minutes

-----
PASSED - On disk timestamp_timeout
```

No matching files were found

5.2.7 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.

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.

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/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3

800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A

NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

```
cmd: sugroup=$(/bin/grep -Pi '\h*auth\h+(?:required|requisite)\h+pam_wheel\so\h+(?:[^\r]+\h+)?((?!
\2)(use_uid\b|group=\H+\b))\h+(?:[^\r]+\h+)?((?!1)(use_uid\b|group=\H+\b))(\h+.*)?$' /etc/pam.d/su | /
bin/awk 'BEGIN { FS = "=" }; { print $2 }'; if [ ! -z $sugroup ]; then /bin/grep $sugroup /etc/group | /bin/awk
'BEGIN { FS = ":" }; { print $4 }' | /bin/awk '{print} END {if (NF == 0) print "pass - group empty"; else print "fail
- group not empty"}'; else echo "fail - sugroup not found in /etc/pam.d/su"; fi expect: pass - group empty
```

Hosts

192.168.40.171

```
The command 'sugroup=$(/bin/grep -Pi '^h*auth\h+(?:required|requisite)\h+pam_wheel\.so\h+(?:[^#\n\r]+\h+)?((?!2)(use_uid\b|group=\H+\b))\h+(?:[^#\n\r]+\h+)?((?!1)(use_uid\b|group=\H+\b))(\h+.*?)?$' /etc/pam.d/su | /bin/awk 'BEGIN { FS = "=" } ; { print $2 }'); if [ ! -z $sugroup ]; then /bin/grep $sugroup /etc/group | /bin/awk 'BEGIN { FS = ":" } ; { print $4 }' | /bin/awk '{print} END {if (NF == 0) print "pass - group empty"; else print "fail - group not empty"}'; else echo "fail - sugroup not found in /etc/pam.d/su"; fi' returned :
```

```
pass - group empty
```


5.3.1.1 Ensure latest version of pam is installed

Info

Updated versions of PAM include additional functionality

To ensure the system has full functionality and access to the options covered by this Benchmark the latest version of libpam-runtime should be installed on the system

Solution

- IF - the version of libpam-runtime on the system is less than version 1.5.3-5 :

Run the following command to update to the latest version of PAM :

```
# apt upgrade libpam-runtime
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s libpam-runtime | /bin/grep -E '(Status:|Version)'

expect: ^Version: ([1-9]|[1-9][0-9])\.[(5-9)|[1-9][0-9])\.[(3-9)|[1-9][0-9])-(5-9)|[1-9][0-9])

Hosts

192.168.40.171

```
The command '/bin/dpkg -s libpam-runtime | /bin/grep -E '(Status:|Version)'' returned :
```

```
Status: install ok installed
```

```
Version: 1.5.3-5ubuntu5.4
```

5.3.1.2 Ensure libpam-modules is installed

Info

Pluggable Authentication Modules for PAM

To ensure the system has full functionality and access to the PAM options covered by this Benchmark

Solution

- IF - the version of libpam-modules on the system is less than version 1.5.3-5 :

Run the following command to update to the latest version of PAM :

```
# apt upgrade libpam-modules
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s libpam-modules | /bin/grep -E '(Status:|Version)'

expect: ^Version: (1\.5\.([3-9]|[1-9][0-9])-(5-9|[1-9][0-9])|1\.([6-9]|[1-9][0-9])\.[2-9]\.|[1-9][0-9]\.)

Hosts

192.168.40.171

```
The command '/bin/dpkg -s libpam-modules | /bin/grep -E '(Status:|Version)'' returned :
```

```
Status: install ok installed
```

```
Version: 1.5.3-5ubuntu5.4
```

5.3.1.3 Ensure libpam-pwquality is installed

Info

libpwquality provides common functions for password quality checking and scoring them based on their apparent randomness. The library also provides a function for generating random passwords with good pronounceability.

This module can be plugged into the password stack of a given service to provide some plug-in strength-checking for passwords. The code was originally based on pam_cracklib module and the module is backwards compatible with its options.

Strong passwords reduce the risk of systems being hacked through brute force methods.

Solution

Run the following command to install libpam-pwquality :

```
# apt install libpam-pwquality
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s libpam-pwquality 2>&1 | /bin/grep -E '(Status:|not installed)'

expect: ^Status: install ok

Hosts

192.168.40.171

```
The command '/bin/dpkg -s libpam-pwquality 2>&1 | /bin/grep -E '(Status:|not installed)''  
returned :  
  
Status: install ok installed
```

5.3.2.1 Ensure pam_unix module is enabled

Info

pam_unix is the standard Unix authentication module. It uses standard calls from the system's libraries to retrieve and set account information as well as authentication. Usually this is obtained from the /etc/passwd and if shadow is enabled, the /etc/shadow file as well.

The account component performs the task of establishing the status of the user's account and password based on the following shadow elements: expire last_change max_change min_change warn_change In the case of the latter, it may offer advice to the user on changing their password or, through the PAM_AUTHTOKEN_REQD return, delay giving service to the user until they have established a new password. The entries listed above are documented in the shadow(5) manual page. Should the user's record not contain one or more of these entries, the corresponding shadow check is not performed.

The authentication component performs the task of checking the users credentials (password). The default action of this module is to not permit the user access to a service if their official password is blank.

The system should only provide access after performing authentication of a user.

Solution

Run the following command to enable the pam_unix module:

```
# pam-auth-update --enable unix
```

Note: If a site specific custom profile is being used in your environment to configure PAM that includes the configuration for the pam_faillock module, enable that module instead

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2

800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.

LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

5.3.2.1 Ensure pam_unix module is enabled

```

-----
PASSED - /etc/pam.d/common-password
Compliant file(s):
    /etc/pam.d/common-password - regex '^h*password\h+[^#\n\r]+\h+pam_unix\.so\b' found - expect
    '^h*password\h+[^#\n\r]+\h+pam_unix\.so\b' found in the following lines:
        28: password[success=1 default=ignore]pam_unix.so obscure yescrypt use_authtok

-----
PASSED - /etc/pam.d/common-account
Compliant file(s):
    /etc/pam.d/common-account - regex '^h*account\h+[^#\n\r]+\h+pam_unix\.so\b' found - expect '^
    \h*account\h+[^#\n\r]+\h+pam_unix\.so\b' found in the following lines:
        17: account[success=1 new_authtok_reqd=done default=ignore]pam_unix.so

-----
PASSED - /etc/pam.d/common-session
Compliant file(s):
    /etc/pam.d/common-session - regex '^h*session\h+[^#\n\r]+\h+pam_unix\.so\b' found - expect '^
    \h*session\h+[^#\n\r]+\h+pam_unix\.so\b' found in the following lines:
        28: sessionrequiredpam_unix.so

-----
PASSED - /etc/pam.d/common-auth
Compliant file(s):
    /etc/pam.d/common-auth - regex '^h*auth\h+[^#\n\r]+\h+pam_unix\.so\b' found - expect '^
    \h*auth\h+[^#\n\r]+\h+pam_unix\.so\b' found in the following lines:
        19: auth    [success=1 default=ignore]    pam_unix.so

```

5.3.2.2 Ensure pam_faillock module is enabled

Info

The pam_faillock.so module maintains a list of failed authentication attempts per user during a specified interval and locks the account in case there were more than the configured number of consecutive failed authentications (this is defined by the deny parameter in the faillock configuration). It stores the failure records into per-user files in the tally directory.

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Solution

Create two pam-auth-update profiles in /usr/share/pam-configs/ :

- Create the faillock profile in /usr/share/pam-configs/ with the following lines:

Name: Enable pam_faillock to deny access Default: yes Priority: 0 Auth-Type: Primary Auth:

[default=die] pam_faillock.so authfail

Example Script:

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

```
{ arr=('Name: Enable pam_faillock to deny access' 'Default: yes' 'Priority: 0' 'Auth-Type: Primary' 'Auth:'  
' [default=die] pam_faillock.so authfail') printf '%s ' "${arr[@]}" > /usr/share/pam-configs/faillock } <xhtml:ol  
start="2"> - Create the faillock_notify profile in /usr/share/pam-configs/ with the following lines:
```

Name: Notify of failed login attempts and reset count upon success Default: yes Priority: 1024 Auth-Type: Primary Auth:

requisite pam_faillock.so preauth Account-Type: Primary Account:

required pam_faillock.so

Example Script:

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

```
{ arr=('Name: Notify of failed login attempts and reset count upon success' 'Default: yes' 'Priority: 1024'  
'Auth-Type: Primary' 'Auth:' ' requisite pam_faillock.so preauth' 'Account-Type: Primary' 'Account:' ' required  
pam_faillock.so') printf '%s ' "${arr[@]}" > /usr/share/pam-configs/faillock_notify }
```

Run the following command to update the common-auth and common-account PAM files with the new profiles:

```
# pam-auth-update --enable <profile_filename>
```

Example:

```
# pam-auth-update --enable faillock # pam-auth-update --enable faillock_notify
```

Note:

- The name used for the file must be used in the pam-auth-update --enable command

- The Name: line should be easily recognizable and understood
- The Priority: Line is important as it effects the order of the lines in the /etc/pam.d/ files
- If a site specific custom profile is being used in your environment to configure PAM that includes the configuration for the pam_faillock module, enable that module instead

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171R3	03.01.01
800-171R3	03.15.01
800-53	AC-1
800-53	AC-2
800-53	AC-2(1)
800-53R5	AC-1
800-53R5	AC-2
800-53R5	AC-2(1)
CN-L3	7.1.3.2(d)
CN-L3	8.1.4.2(e)
CN-L3	8.1.10.6(c)
CSCV7	16.7
CSCV8	6.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.AC-1
CSF	PR.AC-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	GV.OC-03
CSF2.0	GV.OV-01
CSF2.0	GV.PO-01
CSF2.0	GV.PO-02
CSF2.0	GV.SC-03
CSF2.0	ID.IM-01
CSF2.0	ID.IM-02
CSF2.0	ID.IM-03
CSF2.0	PR.AA-01
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.1
ISO-27001-2022	A.5.2
ISO-27001-2022	A.5.4
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18
ISO-27001-2022	A.5.31
ISO-27001-2022	A.5.36
ISO-27001-2022	A.5.37
ISO-27001-2022	A.8.2
ISO-27001-2022	5.2
ISO-27001-2022	5.3
ISO-27001-2022	7.5.1
ISO-27001-2022	7.5.2
ISO-27001-2022	7.5.3
ISO/IEC-27001	A.9.1.1
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-1
ITSG-33	AC-2
ITSG-33	AC-2(1)
LEVEL	1A
NESA	M1.2.2
NIAV2	AM28
NIAV2	AM29
NIAV2	AM30
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - /etc/pam.d/common-account

Compliant file(s):

```
/etc/pam.d/common-account - regex '(?i)^\h*account\h+([\#\n\r]+\h+pam_faillock\.so\b' found -  
expect '(?i)^\h*account\h+([\#\n\r]+\h+pam_faillock\.so\b' found in the following lines:  
26: account required pam_faillock.so
```

PASSED - /etc/pam.d/common-auth authfail

Compliant file(s):

```
/etc/pam.d/common-auth - regex '(?i)^\h*auth\h+([\#\n\r]+\h+pam_faillock\.so\h+([\#\n\r]+\h+)  
\h)?authfail\b' found - expect '(?i)^\h*auth\h+([\#\n\r]+\h+pam_faillock\.so\h+([\#\n\r]+\h+)?  
authfail\b' found in the following lines:  
20: auth[default=die]pam_faillock.so authfail
```

PASSED - /etc/pam.d/common-auth preauth

Compliant file(s):

```
/etc/pam.d/common-auth - regex '(?i)^\h*auth\h+([\#\n\r]+\h+pam_faillock\.so\h+([\#\n\r]+\h+  
+)?preauth\b' found - expect '(?i)^\h*auth\h+([\#\n\r]+\h+pam_faillock\.so\h+([\#\n\r]+\h+)?preauth  
\b' found in the following lines:  
17: authrequiredpam_faillock.so preauth
```

5.3.2.3 Ensure pam_pwquality module is enabled

Info

The pam_pwquality.so module performs password quality checking. This module can be plugged into the password stack of a given service to provide strength-checking for passwords. The code was originally based on pam_cracklib module and the module is backwards compatible with its options.

The action of this module is to prompt the user for a password and check its strength against a system dictionary and a set of rules for identifying poor choices.

The first action is to prompt for a single password, check its strength and then, if it is considered strong, prompt for the password a second time (to verify that it was typed correctly on the first occasion). All being well, the password is passed on to subsequent modules to be installed as the new authentication token.

Use of a unique, complex passwords helps to increase the time and resources required to compromise the password.

Solution

Run the following script to verify the pam_pwquality.so line exists in a pam-auth-update profile:

```
# grep -P -- 'bpam_pwquality.sob' /usr/share/pam-configs/*
```

Output should be similar to:

```
/usr/share/pam-configs/pwquality: requisite pam_pwquality.so retry=3 /usr/share/pam-configs/pwquality:
requisite pam_pwquality.so retry=3
```

- IF - similar output is returned:

Run the following command to update /etc/pam.d/common-password with the returned profile:

```
# pam-auth-update --enable {PROFILE_NAME}
```

Example:

```
# pam-auth-update pwquality
```

- IF - similar output is NOT returned:

Create a pam-auth-update profile in /usr/share/pam-configs/ with the following lines:

Name: Pwquality password strength checking Default: yes Priority: 1024 Conflicts: cracklib Password-Type: Primary Password:

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

Example:

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

```
{ arr=('Name: Pwquality password strength checking' 'Default: yes' 'Priority: 1024' 'Conflicts: cracklib'
'Password-Type: Primary' 'Password:' ' requisite pam_pwquality.so retry=3') printf '%s ' "${arr[@]}" > /usr/
share/pam-configs/pwquality }
```

Run the following command to update /etc/pam.d/common-password with the pwquality profile:

pam-auth-update --enable pwquality

Note:

- The name used for the file must be used in the pam-auth-update --enable command
- The Name: line should be easily recognizable and understood
- The Priority: Line is important as it effects the order of the lines in the /etc/pam.d/ files
- If a site specific custom profile is being used in your environment to configure PAM that includes the configuration for the pam_pwquality module, enable that module instead

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: (?!)\h*password\h+(requisite|required)\h+pam_pwquality\so\b file: /etc/pam.d/common-password regex: (?!)\h*password\h+(requisite|required)\h+pam_pwquality\so\b

Hosts

192.168.40.171

```
Compliant file(s):
/etc/pam.d/common-password - regex '(?i)^\h*password\h+(requisite|required)\h+pam_pwquality
\.so\b' found - expect '(?i)^\h*password\h+(requisite|required)\h+pam_pwquality\.so\b' found in the
following lines:
    25: password      requisite                                pam_pwquality.so local_users_only
retry=3 authtok_type= minlen=14 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1 enforce_for_root
```

5.3.2.4 Ensure pam_pwhistory module is enabled

Info

The pam_pwhistory.so module saves the last passwords for each user in order to force password change history and keep the user from alternating between the same password too frequently.

This module does not work together with kerberos. In general, it does not make much sense to use this module in conjunction with NIS or LDAP since the old passwords are stored on the local machine and are not available on another machine for password history checking.

Use of a unique, complex passwords helps to increase the time and resources required to compromise the password.

Solution

Run the following script to verify the pam_pwquality.so line exists in a pam-auth-update profile:

```
# grep -P -- 'bpam_pwhistory.sob' /usr/share/pam-configs/*
```

Output should be similar to:

```
/usr/share/pam-configs/pwhistory: requisite pam_pwhistory.so remember=24 enforce_for_root  
try_first_pass use_authtok
```

- IF - similar output is returned:

Run the following command to update /etc/pam.d/common-password with the returned profile:

```
# pam-auth-update --enable {PROFILE_NAME}
```

Example:

```
# pam-auth-update pwhistory
```

- IF - similar output is NOT returned:

Create a pwhistory profile in /usr/share/pam-configs/ with the following lines:

Name: pwhistory password history checking Default: yes Priority: 1024 Password-Type: Primary Password:
requisite pam_pwhistory.so remember=24 enforce_for_root try_first_pass use_authtok

Example Script:

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

```
{ arr=('Name: pwhistory password history checking' 'Default: yes' 'Priority: 1024' 'Password-Type: Primary'  
'Password:' ' requisite pam_pwhistory.so remember=24 enforce_for_root try_first_pass use_authtok') printf  
"%s ' "${arr[@]}" " > /usr/share/pam-configs/pwhistory }
```

Run the following command to update /etc/pam.d/common-password with the pwhistory profile:

```
# pam-auth-update --enable pwhistory
```

Note:

- The name used for the file must be used in the pam-auth-update --enable command

- The Name: line should be easily recognizable and understood
- The Priority: Line is important as it effects the order of the lines in the /etc/pam.d/ files
- If a site specific custom profile is being used in your environment to configure PAM that includes the configuration for the pam_pwhistory module, enable that module instead

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: (?i)^\h*password\h+(requisite|required)\h+pam_pwhistory\.so\b file: /etc/pam.d/common-password regex: (?i)^\h*password\h+(requisite|required)\h+pam_pwhistory\.so\b

Hosts

192.168.40.171

```
Compliant file(s):
    /etc/pam.d/common-password - regex '(?i)^\h*password\h+(requisite|required)\h+pam_pwhistory
\so\b' found - expect '(?i)^\h*password\h+(requisite|required)\h+pam_pwhistory\so\b' found in the
following lines:
    27: passwordrequisitepam_pwhistory.so remember=24 enforce_for_root try_first_pass
    use_authtok
```

5.3.3.1.1 Ensure password failed attempts lockout is configured

Info

The deny=<n> option will deny access if the number of consecutive authentication failures for this user during the recent interval exceeds

.

Locking out user IDs after

n

unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Solution

Create or edit the following line in /etc/security/faillock.conf setting the deny option to 5 or less:

deny = 5

Run the following command:

```
# grep -PI -- 'bpam_faillock.soh+([^\# r]+h+)?denyb' /usr/share/pam-configs/*
```

Edit any returned files and remove the deny=<N> arguments from the pam_faillock.so line(s):

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171R3	03.01.01
800-171R3	03.15.01
800-53	AC-1
800-53	AC-2
800-53	AC-2(1)
800-53R5	AC-1
800-53R5	AC-2
800-53R5	AC-2(1)
CN-L3	7.1.3.2(d)
CN-L3	8.1.4.2(e)
CN-L3	8.1.10.6(c)
CSCV7	16.7
CSCV8	6.2
CSF	DE.CM-1
CSF	DE.CM-3

CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.AC-1
CSF	PR.AC-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	GV.OC-03
CSF2.0	GV.OV-01
CSF2.0	GV.PO-01
CSF2.0	GV.PO-02
CSF2.0	GV.SC-03
CSF2.0	ID.IM-01
CSF2.0	ID.IM-02
CSF2.0	ID.IM-03
CSF2.0	PR.AA-01
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.1
ISO-27001-2022	A.5.2
ISO-27001-2022	A.5.4
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18
ISO-27001-2022	A.5.31
ISO-27001-2022	A.5.36
ISO-27001-2022	A.5.37
ISO-27001-2022	A.8.2
ISO-27001-2022	5.2
ISO-27001-2022	5.3
ISO-27001-2022	7.5.1
ISO-27001-2022	7.5.2
ISO-27001-2022	7.5.3
ISO/IEC-27001	A.9.1.1
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-1
ITSG-33	AC-2
ITSG-33	AC-2(1)
LEVEL	1A
NESA	M1.2.2
NIAV2	AM28

NIAV2	AM29
NIAV2	AM30
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - /etc/security/faillock.conf

Compliant file(s):

/etc/security/faillock.conf - regex '(?i)^\h*deny\h*=\h*[1-5]\b' found - expect '(?i)^\h*deny
\h*=\h*[1-5]\b' found in the following lines:
63: deny = 5

PASSED - /etc/pam.d/common-auth
No matching files were found

5.3.3.1.2 Ensure password unlock time is configured

Info

`unlock_time=<n>` - The access will be re-enabled after

seconds after the lock out. The value 0 has the same meaning as value never - the access will not be re-enabled without resetting the faillock entries by the `faillock(8)` command.

Note:

- The default directory that `pam_faillock` uses is usually cleared on system boot so the access will be also re-enabled after system reboot. If that is undesirable a different tally directory must be set with the `dir` option.
- It is usually undesirable to permanently lock out users as they can become easily a target of denial of service attack unless the usernames are random and kept secret to potential attackers.
- The maximum configurable value for `unlock_time` is 604800

Locking out user IDs after

n

unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Solution

Set password unlock time to conform to site policy. `unlock_time` should be 0 (never), or 900 seconds or greater.

Edit `/etc/security/faillock.conf` and update or add the following line:

```
unlock_time = 900
```

Run the following command: remove the `unlock_time` argument from the `pam_faillock.so` module in the PAM files:

```
# grep -PI -- 'bpam_faillock.soh+([^\# r]+h+)?unlock_timeb' /usr/share/pam-configs/*
```

Edit any returned files and remove the `unlock_time=<N>` argument from the `pam_faillock.so` line(s):

Impact:

Use of `unlock_time=0` may allow an attacker to cause denial of service to legitimate users. This will also require a systems administrator with elevated privileges to unlock the account.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171R3	03.01.01
800-171R3	03.15.01

800-53	AC-1
800-53	AC-2
800-53	AC-2(1)
800-53R5	AC-1
800-53R5	AC-2
800-53R5	AC-2(1)
CN-L3	7.1.3.2(d)
CN-L3	8.1.4.2(e)
CN-L3	8.1.10.6(c)
CSCV7	16.7
CSCV8	6.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.AC-1
CSF	PR.AC-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	GV.OC-03
CSF2.0	GV.OV-01
CSF2.0	GV.PO-01
CSF2.0	GV.PO-02
CSF2.0	GV.SC-03
CSF2.0	ID.IM-01
CSF2.0	ID.IM-02
CSF2.0	ID.IM-03
CSF2.0	PR.AA-01
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.1
ISO-27001-2022	A.5.2
ISO-27001-2022	A.5.4
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18
ISO-27001-2022	A.5.31
ISO-27001-2022	A.5.36
ISO-27001-2022	A.5.37
ISO-27001-2022	A.8.2

ISO-27001-2022	5.2
ISO-27001-2022	5.3
ISO-27001-2022	7.5.1
ISO-27001-2022	7.5.2
ISO-27001-2022	7.5.3
ISO/IEC-27001	A.9.1.1
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-1
ITSG-33	AC-2
ITSG-33	AC-2(1)
LEVEL	1A
NESA	M1.2.2
NIAV2	AM28
NIAV2	AM29
NIAV2	AM30
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

```
-----
PASSED - /etc/security/faillock.conf
Compliant file(s):
    /etc/security/faillock.conf - regex '(?i)^\h*unlock_time\h*=' found - expect '(?i)^\h*unlock_time\h*=\h*(0|9[0-9][0-9]|[1-9][0-9]{3,})\b' found in the following lines:
        65: unlock_time = 900

-----
PASSED - /etc/pam.d/common-auth
No matching files were found
```

5.3.3.2.1 Ensure password number of changed characters is configured

Info

The pwquality difok option sets the number of characters in a password that must not be present in the old password.

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Solution

Create or modify a file ending inconf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line to set difok to 2 or more. Ensure setting conforms to local site policy:

Example:

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

{ sed -ri 's/^s*difoks*=/# &/' /etc/security/pwquality.conf [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir /etc/security/pwquality.conf.d/ printf '%s' "difok = 2" > /etc/security/pwquality.conf.d/50-pwdifok.conf }
```

Run the following command:

```
# grep -PI -- 'bpam_pwquality.soh+([^\# r]+h+)?difokb' /usr/share/pam-configs/*
```

Edit any returned files and remove the difok argument from the pam_pwquality.so line(s):

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

```
-----
PASSED - pwquality - difok
Compliant file(s):
    /etc/security/pwquality.conf - regex '(?i)^\h*difok\h*=' found - expect '(?i)^\h*difok\h*=
\h*([2-9]|[1-9][0-9]+)\b' found in the following lines:
    6: difok = 2
-----
PASSED - /etc/pam.d/common-password
No matching files were found
```

5.3.3.2.2 Ensure minimum password length is configured

Info

The minimum password length setting determines the lower number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "passphrase" is a better term than "password".

The minlen option sets the minimum acceptable size for the new password (plus one if credits are not disabled which is the default). Cannot be set to lower value than 6.

Strong passwords help protect systems from password attacks. Types of password attacks include dictionary attacks, which attempt to use common words and phrases, and brute force attacks, which try every possible combination of characters. Also attackers may try to obtain the account database so they can use tools to discover the accounts and passwords.

Solution

Create or modify a file ending inconff in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line to set password length of 14 or more characters. Ensure that password length conforms to local site policy:

Example:

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

```
{ sed -ri 's/^s*minlen*=/# &/' /etc/security/pwquality.conf [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir /etc/security/pwquality.conf.d/ printf '
```

```
%s' "minlen = 14" > /etc/security/pwquality.conf.d/50-pwlength.conf }
```

Run the following command:

```
# grep -PI -- 'bpam_pwquality.soh+([^\# r]+h+)?minlenb' /usr/share/pam-configs/*
```

Edit any returned files and remove the minlen argument from the pam_pwquality.so line(s):

Impact:

In general, it is true that longer passwords are better (harder to crack), but it is also true that forced password length requirements can cause user behavior that is predictable and undesirable. For example, requiring users to have a minimum 16-character password may cause them to choose repeating patterns like fourfourfourfour or passwordpassword that meet the requirement but aren't hard to guess. Additionally, length requirements increase the chances that users will adopt other insecure practices, like writing them down, re-using them or storing them unencrypted in their documents.

Having a reasonable minimum length with no maximum character limit increases the resulting average password length used (and therefore the strength).6

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - /etc/pam.d/common-password
Compliant file(s):

```
/etc/pam.d/common-password - regex '^h*passwordh+(requisite|required|sufficient)h+
+pam_pwquality.so\h+(\^[#\r]+\h+)?minlen\h*=' found - expect '^h*passwordh+(requisite|required|
sufficient)h+pam_pwquality.so\h+(\^[#\r]+\h+)?minlen\h*=\h*(1[4-9]|[2-9][0-9]|[1-9][0-9]{2,})\b'
found in the following lines:
    25: password      requisite                                pam_pwquality.so local_users_only
    retry=3 authtok_type= minlen=14 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1 enforce_for_root
```

PASSED - pwquality - minlen
Compliant file(s):

```
/etc/security/pwquality.conf - regex '(?i)^\h*minlen\h*=' found - expect '(?i)^\h*minlen\h*=
\h*(1[4-9]|[2-9][0-9]|[1-9][0-9]{2,})\b' found in the following lines:
```

```
11: minlen = 14
```

5.3.3.2.3 Ensure password complexity is configured

Info

Password complexity can be set through:

- minclass - The minimum number of classes of characters required in a new password. (digits, uppercase, lowercase, others). e.g. minclass = 4 requires digits, uppercase, lower case, and special characters.
- dcredit - The maximum credit for having digits in the new password. If less than 0 it is the minimum number of digits in the new password. e.g. dcredit = -1 requires at least one digit
- ucredit - The maximum credit for having uppercase characters in the new password. If less than 0 it is the minimum number of uppercase characters in the new password. e.g. ucredit = -1 requires at least one uppercase character
- ocredit - The maximum credit for having other characters in the new password. If less than 0 it is the minimum number of other characters in the new password. e.g. ocredit = -1 requires at least one special character
- lcredit - The maximum credit for having lowercase characters in the new password. If less than 0 it is the minimum number of lowercase characters in the new password. e.g. lcredit = -1 requires at least one lowercase character

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

Requiring at least one non-alphabetic character increases the search space beyond pure dictionary words, which makes the resulting password harder to crack.

Forcing users to choose an excessively complex password, e.g. some combination of upper-case, lower-case, numbers, and special characters, has a negative impact. It places an extra burden on users and many will use predictable patterns (for example, a capital letter in the first position, followed by lowercase letters, then one or two numbers, and a "special character" at the end). Attackers know this, so dictionary attacks will often contain these common patterns and use the most common substitutions like, \$ for s, @ for a, 1 for l, 0 for o.

Solution

Run the following command:

```
# grep -PI -- 'bpam_pwquality.soh+([^\# r]+h+)?(minclass|[dulo]credit)b' /usr/share/pam-configs/*
```

Edit any returned files and remove the minclass dcredit ucredit lcredit and ocredit arguments from the pam_pwquality.so line(s)

Create or modify a file ending inconf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line(s) to set complexity according to local site policy:

- minclass = _N_
- dcredit = _N_ # Value should be either 0 or a number proceeded by a minus (-) symbol
- ucredit = -1 # Value should be either 0 or a number proceeded by a minus (-) symbol
- ocredit = -1 # Value should be either 0 or a number proceeded by a minus (-) symbol
- lcredit = -1 # Value should be either 0 or a number proceeded by a minus (-) symbol

Example 1 - Set minclass = 3 :


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

```
{ sed -ri 's/^s*minclasss*=/# &/' /etc/security/pwquality.conf sed -ri 's/^s*[dulo]credits*=/# &/' /etc/security/pwquality.conf [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir /etc/security/pwquality.conf.d/ printf '%s' "minclass = 3" > /etc/security/pwquality.conf.d/50-pwcomplexity.conf }
```

Example 2 - set dcredit = -1 ucredit = -1 and lcredit = -1 :

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

```
{ sed -ri 's/^s*minclasss*=/# &/' /etc/security/pwquality.conf sed -ri 's/^s*[dulo]credits*=/# &/' /etc/security/pwquality.conf [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir /etc/security/pwquality.conf.d/ printf '%s' "dcredit = -1" "ucredit = -1" "lcredit = -1" > /etc/security/pwquality.conf.d/50-pwcomplexity.conf }
```

Impact:

Passwords that are too complex in nature make it harder for users to remember, leading to bad practices. In addition, composition requirements provide no defense against common attack types such as social engineering or insecure storage of passwords

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1M
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - ocredit

Compliant file(s):

/etc/security/pwquality.conf - regex '^[\s]*ocredit[\s]*=' found - expect
'^[\s]*ocredit[\s]*=[\s]*-[1-9][\s]*\$' found in the following lines:
30: ocredit = -1

PASSED - ucredit

Compliant file(s):

/etc/security/pwquality.conf - regex '^[\s]*ucredit[\s]*=' found - expect
'^[\s]*ucredit[\s]*=[\s]*-[1-9][\s]*\$' found in the following lines:
20: ucredit = -1

PASSED - lcredit

Compliant file(s):

/etc/security/pwquality.conf - regex '^[\s]*lcredit[\s]*=' found - expect
'^[\s]*lcredit[\s]*=[\s]*-[1-9][\s]*\$' found in the following lines:
25: lcredit = -1

PASSED - dcredit

Compliant file(s):

/etc/security/pwquality.conf - regex '^[\s]*dcredit[\s]*=' found - expect
'^[\s]*dcredit[\s]*=[\s]*-[1-9][\s]*\$' found in the following lines:
15: dcredit = -1

5.3.3.2.4 Ensure password same consecutive characters is configured

Info

The pwquality maxrepeat option sets the maximum number of allowed same consecutive characters in a new password.

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Solution

Create or modify a file ending inconf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line to set maxrepeat to 3 or less and not 0 Ensure setting conforms to local site policy:

Example:

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

```
{ sed -ri 's/^s*maxrepeats*=/# &/' /etc/security/pwquality.conf [ ! -d /etc/security/pwquality.conf.d/ ] &&
mkdir /etc/security/pwquality.conf.d/ printf '
%s' "maxrepeat = 3" > /etc/security/pwquality.conf.d/50-pwrepeat.conf }
```

Run the following command:

```
# grep -PI -- 'bpam_pwquality.soh+([^\# r]+h+)?maxrepeatb' /usr/share/pam-configs/*
```

Edit any returned files and remove the maxrepeat argument from the pam_pwquality.so line(s):

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - pwquality - maxrepeat

Compliant file(s):

/etc/security/pwquality.conf - regex '(?i)^\h*maxrepeat\h*' found - expect '(?i)^\h*maxrepeat
\h*=\h*[1-3]\b' found in the following lines:
38: maxrepeat = 3

PASSED - /etc/pam.d/common-password

No matching files were found

5.3.3.2.5 Ensure password maximum sequential characters is configured

Info

The pwquality maxsequence option sets the maximum length of monotonic character sequences in the new password. Examples of such sequence are 12345 or fedcb The check is disabled if the value is 0

Note: Most such passwords will not pass the simplicity check unless the sequence is only a minor part of the password.

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Solution

Create or modify a file ending inconf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line to set maxsequence to 3 or less and not 0 Ensure setting conforms to local site policy:

Example:

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

{ sed -ri 's/^s*maxsequences*=/# &/' /etc/security/pwquality.conf [ ! -d /etc/security/pwquality.conf.d/ ] &&
mkdir /etc/security/pwquality.conf.d/ printf '
%s' "maxsequence = 3" > /etc/security/pwquality.conf.d/50-pwmaxsequence.conf }
```

Run the following command:

```
# grep -PI -- 'bpam_pwquality.soh+([\^# r]+h+)?maxsequenceb' /usr/share/pam-configs/*
```

Edit any returned files and remove the maxsequence argument from the pam_pwquality.so line(s):

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1

CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - pwquality - maxsequence

Compliant file(s):

/etc/security/pwquality.conf - regex '(?i)^\h*maxsequence\h*=' found - expect '(?i)^\h*maxsequence\h*=\h*[1-3]\b' found in the following lines:
82: maxsequence = 3

PASSED - /etc/pam.d/common-password

No matching files were found

5.3.3.2.6 Ensure password dictionary check is enabled

Info

The pwquality dictcheck option sets whether to check for the words from the cracklib dictionary.

If the operating system allows the user to select passwords based on dictionary words, this increases the chances of password compromise by increasing the opportunity for successful guesses, and brute-force attacks.

Solution

Edit any file ending inconf in the /etc/security/pwquality.conf.d/ directory and/or the file /etc/security/pwquality.conf and comment out or remove any instance of dictcheck = 0 :

Example:

```
# sed -ri 's/^s*dictchecks*=/# &/' /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

Run the following command:

```
# grep -PI -- 'bpam_pwquality.soh+([^\# r]+h+)?dictcheckb' /usr/share/pam-configs/*
```

Edit any returned files and remove the dictcheck argument from the pam_pwquality.so line(s)

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A

NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - pwquality - dictcheck

The following file(s) do not contain "(?i)^\h*dictcheck\h*=\h*0\b":
 /etc/security/pwquality.conf

PASSED - /etc/pam.d/common-password

The following file(s) do not contain "(?i)^\h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([\#\r]+\h+)?dictcheck\h*=\h*0\b":
 /etc/pam.d/common-password

5.3.3.2.7 Ensure password quality checking is enforced

Info

The pam_pwquality module can be configured to either reject a password if it fails the checks, or only print a warning.

This is configured by setting the enforcing=<N> argument. If nonzero, a password will be rejected if it fails the checks, otherwise only a warning message will be provided.

This setting applies only to the pam_pwquality module and possibly other applications that explicitly change their behavior based on it. It does not affect pwmake(1) and pwscore(1).

Strong passwords help protect systems from password attacks. Types of password attacks include dictionary attacks, which attempt to use common words and phrases, and brute force attacks, which try every possible combination of characters. Also attackers may try to obtain the account database so they can use tools to discover the accounts and passwords.

Solution

Run the following command:

```
# grep -PI -- 'bpam_pwquality.soh+([^\# r]+h+)?enforcing=0b' /usr/share/pam-configs/*
```

Edit any returned files and remove the enforcing=0 argument from the pam_pwquality.so line(s)

Edit /etc/security/pwquality.conf and all files ending inconf in the /etc/security/pwquality.conf.d/ directory and remove or comment out any line containing the enforcing = 0 argument:

Example:

```
# sed -ri 's/^s*enforcings*=s*0/# &/' /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

```
-----
PASSED - /etc/pam.d/common-password
The following file(s) do not contain "(?i)^\h*password\h+(requisite|required|sufficient)\h
+pam_pwquality\.so\h+([\r]+)\h+)?enforcing\h*=\h*0\b":
    /etc/pam.d/common-password
```

```
-----
PASSED - pwquality - enforcing
The following file(s) do not contain "(?i)^\h*enforcing\h*=\h*0\b":
    /etc/security/pwquality.conf
```

5.3.3.2.8 Ensure password quality is enforced for the root user

Info

If the `pwquality enforce_for_root` option is enabled, the module will return error on failed check even if the user changing the password is root.

This option is off by default which means that just the message about the failed check is printed but root can change the password anyway.

Note: The root is not asked for an old password so the checks that compare the old and new password are not performed.

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Solution

Edit or add the following line in a `*.conf` file in `/etc/security/pwquality.conf.d` or in `/etc/security/pwquality.conf` :

Example:

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

```
{ [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir /etc/security/pwquality.conf.d/ printf '%s ' "enforce_for_root" > /etc/security/pwquality.conf.d/50-pwroot.conf }
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: (?i)^\h*enforce_for_root\b file: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
min_occurrences: 1 regex: (?i)^\h*enforce_for_root\b string_required: NO

Hosts

192.168.40.171

```
Compliant file(s):
    /etc/security/pwquality.conf - regex '(?i)^\h*enforce_for_root\b' found - expect '(?i)^\h*enforce_for_root\b' found in the following lines:
        85: enforce_for_root
```

5.3.3.3.1 Ensure password history remember is configured

Info

The `/etc/security/opasswd` file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords. The number of passwords remembered is set via the `remember` argument value in set for the `pam_pwhistory` module.

- `remember=<N>` - `<N>` is the number of old passwords to remember

Requiring users not to reuse their passwords make it less likely that an attacker will be able to guess the password or use a compromised password.

Note: These change only apply to accounts configured on the local system.

Solution

Run the following command:

```
# awk 'Password-Type:/{ f = 1;next } /-Type:/{ f = 0 } f {if (/pam_pwhistory.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files and edit or add the `remember=` argument, with a value of 24 or more, that meets local site policy to the `pam_pwhistory` line in the Password section:

Example File:

Name: pwhistory password history checking Default: yes Priority: 1024 Password-Type: Primary Password: requisite pam_pwhistory.so remember=24 enforce_for_root try_first_pass use_authtok # <- **ensure line includes remember=<N>**

Run the following command to update the files in the `/etc/pam.d/` directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

Example:

```
# pam-auth-update --enable pwhistory
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2

CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: (?:)^\h*password\h+(requisite|required|sufficient)\h+pam_pwhistory\.so\h+([\#\r]+\h+)?
remember=(2[4-9]|[3-9][0-9]|[1-9][0-9]{2,})\b file: /etc/pam.d/common-password regex: (?:)^\h*password\h+
(requisite|required|sufficient)\h+pam_pwhistory\.so\h+([\#\r]+\h+)?remember=

Hosts

192.168.40.171

```
Compliant file(s):
/etc/pam.d/common-password - regex '(?:)^\h*password\h+(requisite|required|sufficient)\h
+pam_pwhistory\.so\h+([\#\r]+\h+)?remember=' found - expect '(?:)^\h*password\h+(requisite|required|
sufficient)\h+pam_pwhistory\.so\h+([\#\r]+\h+)?remember=(2[4-9]|[3-9][0-9]|[1-9][0-9]{2,})\b' found
in the following lines:
    27: passwordrequisitepam_pwhistory.so remember=24 enforce_for_root try_first_pass
    use_authtok
```

5.3.3.3.2 Ensure password history is enforced for the root user

Info

If the `pwhistory enforce_for_root` option is enabled, the module will enforce password history for the root user as well

Requiring users not to reuse their passwords make it less likely that an attacker will be able to guess the password or use a compromised password

Note: These change only apply to accounts configured on the local system.

Solution

Run the following command:

```
# awk 'Password-Type:{ f = 1;next } /-Type:{ f = 0 } f {if (/pam_pwhistory.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files and add the `enforce_for_root` argument to the `pam_pwhistory` line in the Password section:

Example File:

Name: `pwhistory` password history checking Default: `yes` Priority: `1024` Password-Type: `Primary` Password: `requisite pam_pwhistory.so remember=24 enforce_for_root try_first_pass use_authtok # <- **ensure line includes enforce_for_root**`

Run the following command to update the files in the `/etc/pam.d/` directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

Example:

```
# pam-auth-update --enable pwhistory
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: (?:)^\h*password\h+[^#\r]+\h+pam_pwhistory\.so\h+([^\#\n\r]+\h+)?enforce_for_root\b file: /etc/pam.d/common-password regex: (?:)^\h*password\h+[^#\r]+\h+pam_pwhistory\.so\h+([^\#\n\r]+\h+)?enforce_for_root\b

Hosts

192.168.40.171

```
Compliant file(s):
/etc/pam.d/common-password - regex '(?:)^\h*password\h+[^#\n\r]+\h+pam_pwhistory\.so\h+([^\#\n\r]+\h+)?enforce_for_root\b' found - expect '(?:)^\h*password\h+[^#\n\r]+\h+pam_pwhistory\.so\h+([^\#\n\r]+\h+)?enforce_for_root\b' found in the following lines:
    27: passwordrequisitepam_pwhistory.so remember=24 enforce_for_root try_first_pass
    use_authtok
```


5.3.3.3 Ensure pam_pwhistory includes use_authtok

Info

use_authtok - When password changing enforce the module to set the new password to the one provided by a previously stacked password module

use_authtok allows multiple pam modules to confirm a new password before it is accepted.

Solution

Run the following command:

```
# awk 'Password-Type:{ f = 1;next } /-Type:{ f = 0 } f {if (/pam_pwhistory.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files and add the use_authtok argument to the pam_pwhistory line in the Password section:

Example File:

Name: pwhistory password history checking Default: yes Priority: 1024 Password-Type: Primary Password: requisite pam_pwhistory.so remember=24 enforce_for_root try_first_pass use_authtok # <- **ensure line includes use_authtok**

Run the following command to update the files in the /etc/pam.d/ directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

Example:

```
# pam-auth-update --enable pwhistory
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171	3.13.16
800-171R3	03.05.07
800-171R3	03.13.08
800-53	IA-5(1)
800-53	SC-28
800-53	SC-28(1)
800-53R5	IA-5(1)
800-53R5	SC-28
800-53R5	SC-28(1)
CN-L3	8.1.4.7(b)

CN-L3	8.1.4.8(b)
CSCV7	16.4
CSCV8	3.11
CSF	PR.AC-1
CSF	PR.DS-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
CSF2.0	PR.DS-01
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(d)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO-27001-2022	A.5.33
ITSG-33	IA-5(1)
ITSG-33	SC-28
ITSG-33	SC-28a.
ITSG-33	SC-28(1)
LEVEL	1A
NESA	T5.2.3
PCI-DSSV3.2.1	3.4
PCI-DSSV4.0	3.3.2
PCI-DSSV4.0	3.5.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1
TBA-FIISB	28.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: (?i)^\h*password\h+(requisite|required|sufficient)\h+pam_pwhistory\so(\h+[\^#\r]+)?\h+use_authtok\b file: /etc/pam.d/common-password regex: (?i)^\h*password\h+(requisite|required|sufficient)\h+pam_pwhistory\so(\h+[\^#\r]+)?\h+use_authtok\b

Hosts

192.168.40.171

```
Compliant file(s):
    /etc/pam.d/common-password - regex '(?i)^\h*password\h+(requisite|required|sufficient)\h
+pam_pwhistory\.so(\h+[^#\n\r]+)?\h+use_authtok\b' found - expect '(?i)^\h*password\h+(requisite|
required|sufficient)\h+pam_pwhistory\.so(\h+[^#\n\r]+)?\h+use_authtok\b' found in the following
lines:
    27: passwordrequisitepam_pwhistory.so remember=24 enforce_for_root try_first_pass
    use_authtok
```

5.3.3.4.1 Ensure pam_unix does not include nullok

Info

The nullok argument overrides the default action of pam_unix.so to not permit the user access to a service if their official password is blank.

Using a strong password is essential to helping protect personal and sensitive information from unauthorized access

Solution

Run the following command:

```
# grep -PH -- '^h*([^\# r]+h+)?pam_unix.soh+([^\# r]+h+)?nullok' /usr/share/pam-configs/*
```

Edit any files returned and remove the nullok argument for the pam_unix lines

Example File:

Name: Unix authentication Default: yes Priority: 256 Auth-Type: Primary Auth:

[success=end default=ignore] pam_unix.so try_first_pass # <- **ensure line does not include nullok nullok** Auth-Initial:

[success=end default=ignore] pam_unix.so # <- **ensure line does not include nullok nullok** Account-Type: Primary Account:

[success=end new_authtok_reqd=done default=ignore] pam_unix.so Account-Initial:

[success=end new_authtok_reqd=done default=ignore] pam_unix.so Session-Type: Additional Session: required pam_unix.so Session-Initial:

required pam_unix.so Password-Type: Primary Password:

[success=end default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt Password-Initial:

[success=end default=ignore] pam_unix.so obscure yescrypt

Run the following command to update the files in the /etc/pam.d/ directory:

```
# pam-auth-update --enable <EDITED_PROFILE_NAME>
```

Example:

```
# pam-auth-update --enable unix
```

Note: If custom files are being used, the corresponding files in /etc/pam.d/ would need to be edited directly, and the pam-auth-update --enable <EDITED_PROFILE_NAME> command skipped

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171

3.5.2

800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - /etc/pamd./common-session-noninteractive nullok

The following file(s) do not contain "(?i)^\h*\h*[^#\n\r]+\h+pam_unix\.so\b[^\n\r]+nullok\b":
/etc/pamd./common-session-noninteractive

PASSED - /etc/pamd./common-password nullok

The following file(s) do not contain "(?i)^\h*\h*[^#\n\r]+\h+pam_unix\.so\b[^\n\r]+nullok\b":
/etc/pamd./common-password

PASSED - /etc/pamd./common-auth nullok

The following file(s) do not contain "(?i)^\h*\h*[^#\n\r]+\h+pam_unix\.so\b[^\n\r]+nullok\b":
/etc/pamd./common-auth

PASSED - /etc/pamd./common-account nullok

```
The following file(s) do not contain "(?i)^\h*\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+nullok\b":  
    /etc/pam.d/common-account
```

```
-----
```

```
PASSED - /etc/pamd./common-session nullok
```

```
The following file(s) do not contain "(?i)^\h*\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+nullok\b":  
    /etc/pam.d/common-session
```

5.3.3.4.2 Ensure pam_unix does not include remember

Info

The `remember=n` argument saves the last `n` passwords for each user in `/etc/security/opasswd` in order to force password change history and keep the user from alternating between the same password too frequently. The MD5 password hash algorithm is used for storing the old passwords. Instead of this option the `pam_pwhistory` module should be used. The `pam_pwhistory` module saves the last `n` passwords for each user in `/etc/security/opasswd` using the password hash algorithm set on the `pam_unix` module. This allows for the `yescrypt` or `sha512` hash algorithm to be used.

The `remember=n` argument should be removed to ensure a strong password hashing algorithm is being used. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local user's old passwords stored in `/etc/security/opasswd`.

Solution

Run the following command:

```
# grep -PH -- '^h*([^\# r]+h+)?pam_unix.soh+([^\# r]+h+)?rememberb' /usr/share/pam-configs/*
```

Edit any files returned and remove the `remember=<N>` argument for the `pam_unix` lines

Example output:

```
[success=end default=ignore] pam_unix.so obscure use_authok try_first_pass yescrypt remember=5 # **<-
remove remember=<N>** [success=end default=ignore] pam_unix.so obscure yescrypt remember=5 #
**<- remove remember=<N>**
```

Run the following command to update the files in the `/etc/pam.d/` directory:

```
# pam-auth-update --enable <EDITED_PROFILE_NAME>
```

Example:

```
# pam-auth-update --enable unix
```

Note: If custom files are being used, the corresponding files in `/etc/pam.d/` would need to be edited directly, and the `pam-auth-update --enable <EDITED_PROFILE_NAME>` command skipped

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2

CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

```
-----
PASSED - /etc/pamd./common-session remember=
The following file(s) do not contain "(?i)^\h*\h*[^#\n\r]+\h+pam_unix\.so\b[^\n\r]+remember=\b":
/etc/pam.d/common-session
```

```
-----
PASSED - /etc/pamd./common-password remember=
The following file(s) do not contain "(?i)^\h*\h*[^#\n\r]+\h+pam_unix\.so\b[^\n\r]+remember=\b":
/etc/pam.d/common-password
```

```
-----
PASSED - /etc/pamd./common-session-noninteractive remember=
The following file(s) do not contain "(?i)^\h*\h*[^#\n\r]+\h+pam_unix\.so\b[^\n\r]+remember=\b":
/etc/pam.d/common-session-noninteractive
```

```
-----
PASSED - /etc/pamd./common-auth remember=
The following file(s) do not contain "(?i)^\h*\h*[^#\n\r]+\h+pam_unix\.so\b[^\n\r]+remember=\b":
/etc/pam.d/common-auth
```

```
-----
PASSED - /etc/pamd./common-account remember=
The following file(s) do not contain "(?i)^\h*\h*[^#\n\r]+\h+pam_unix\.so\b[^\n\r]+remember=\b":
/etc/pam.d/common-account
```


5.3.3.4.3 Ensure pam_unix includes a strong password hashing algorithm

Info

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.

The pam_unix module can be configured to use one of the following hashing algorithms for user's passwords:

- md5 - When a user changes their password next, encrypt it with the MD5 algorithm.
- bigcrypt - When a user changes their password next, encrypt it with the DEC C2 algorithm.
- sha256 - When a user changes their password next, encrypt it with the SHA256 algorithm. The SHA256 algorithm must be supported by the crypt(3) function.
- sha512 - When a user changes their password next, encrypt it with the SHA512 algorithm. The SHA512 algorithm must be supported by the crypt(3) function.
- blowfish - When a user changes their password next, encrypt it with the blowfish algorithm. The blowfish algorithm must be supported by the crypt(3) function.
- gost-yescrypt - When a user changes their password next, encrypt it with the gost-yescrypt algorithm. The gost-yescrypt algorithm must be supported by the crypt(3) function.
- yescrypt - When a user changes their password next, encrypt it with the yescrypt algorithm. The yescrypt algorithm must be supported by the crypt(3) function.

The SHA-512 and yescrypt algorithms provide a stronger hash than other algorithms used by Linux for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local user passwords.

Note: These changes only apply to the local system.

Solution

Run the following command:

```
# awk 'Password-Type:{ f = 1;next } /-Type:{ f = 0 } f {if (/pam_unix.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files and edit or add a strong hashing algorithm, either sha512 or yescrypt, that meets local site policy to the pam_unix lines in the Password section:

Example File:

```
Name: Unix authentication Default: yes Priority: 256 Auth-Type: Primary # <- Start of "Auth" section Auth:
[success=end default=ignore] pam_unix.so try_first_pass Auth-Initial:
[success=end default=ignore] pam_unix.so Account-Type: Primary # <- Start of "Account" section Account:
[success=end new_authtok_reqd=done default=ignore] pam_unix.so Account-Initial:
[success=end new_authtok_reqd=done default=ignore] pam_unix.so Session-Type: Additional # <- Start of
"Session" section Session:
required pam_unix.so Session-Initial:
required pam_unix.so Password-Type: Primary # <- Start of "Password" section Password:
```

[success=end default=ignore] pam_unix.so obscure use_authok try_first_pass yescrypt # <- **ensure hashing algorithm is either sha512 or yescrypt** Password-Initial:

[success=end default=ignore] pam_unix.so obscure yescrypt # <- **ensure hashing algorithm is either sha512 or yescrypt**

Run the following command to update the files in the /etc/pam.d/ directory:

pam-auth-update --enable <MODIFIED_PROFILE_NAME>

Example:

pam-auth-update --enable unix

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171	3.13.16
800-171R3	03.05.07
800-171R3	03.13.08
800-53	IA-5(1)
800-53	SC-28
800-53	SC-28(1)
800-53R5	IA-5(1)
800-53R5	SC-28
800-53R5	SC-28(1)
CN-L3	8.1.4.7(b)
CN-L3	8.1.4.8(b)
CSCV7	16.4
CSCV8	3.11
CSF	PR.AC-1
CSF	PR.DS-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
CSF2.0	PR.DS-01
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(d)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.16

ISO-27001-2022	A.5.17
ISO-27001-2022	A.5.33
ITSG-33	IA-5(1)
ITSG-33	SC-28
ITSG-33	SC-28a.
ITSG-33	SC-28(1)
LEVEL	1A
NESA	T5.2.3
PCI-DSSV3.2.1	3.4
PCI-DSSV4.0	3.3.2
PCI-DSSV4.0	3.5.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1
TBA-FIISB	28.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: (?i)^\h*password\h+([\^# \r]+\h+pam_unix\.so\h+([\^# \r]+\h+)?(SHA512|YESCRYPT)\b file: /etc/pam.d/common-password regex: (?i)^\h*password\h+([\^# \r]+\h+pam_unix\.so\h+([\^# \r]+\h+)?(SHA512|YESCRYPT)\b

Hosts

192.168.40.171

```
Compliant file(s):
/etc/pam.d/common-password - regex '(?i)^\h*password\h+([\^#\n\r]+\h+pam_unix\.so\h+([\^#\n\r]+\h+)?(SHA512|YESCRYPT)\b' found - expect '(?i)^\h*password\h+([\^#\n\r]+\h+pam_unix\.so\h+([\^#\n\r]+\h+)?(SHA512|YESCRYPT)\b' found in the following lines:
28: password[success=1 default=ignore]pam_unix.so obscure yescrypt use_authtok
```

5.3.3.4.4 Ensure pam_unix includes use_authtok

Info

use_authtok - When password changing enforce the module to set the new password to the one provided by a previously stacked password module

use_authtok allows multiple pam modules to confirm a new password before it is accepted.

Solution

Run the following command:

```
# awk 'Password-Type:{ f = 1;next } /-Type:{ f = 0 } f {if (/pam_unix.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files add use_authtok to the pam_unix line in the Password section under Password: subsection:

Note: The if the file's Password section includes a Password-Initial: subsection, use_authtok should not be added to the pam_unix line in the Password-Initial: subsection

Example File:

```
Name: Unix authentication Default: yes Priority: 256 Auth-Type: Primary # <- Start of "Auth" section Auth:
[success=end default=ignore] pam_unix.so try_first_pass Auth-Initial:
[success=end default=ignore] pam_unix.so Account-Type: Primary # <- Start of "Account" section Account:
[success=end new_authtok_reqd=done default=ignore] pam_unix.so Account-Initial:
[success=end new_authtok_reqd=done default=ignore] pam_unix.so Session-Type: Additional # <- Start of
"Session" section Session:
required pam_unix.so Session-Initial:
required pam_unix.so Password-Type: Primary # <- Start of "Password" section Password:
[success=end default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt # <- **ensure line
includes use_authtok** Password-Initial:
[success=end default=ignore] pam_unix.so obscure yescrypt # <- **Password-Initial: subsection does not
include use_authtok
```

Run the following command to update the files in the /etc/pam.d/ directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

Example:

```
# pam-auth-update --enable unix
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171	3.13.16
800-171R3	03.05.07
800-171R3	03.13.08
800-53	IA-5(1)
800-53	SC-28
800-53	SC-28(1)
800-53R5	IA-5(1)
800-53R5	SC-28
800-53R5	SC-28(1)
CN-L3	8.1.4.7(b)
CN-L3	8.1.4.8(b)
CSCV7	16.4
CSCV8	3.11
CSF	PR.AC-1
CSF	PR.DS-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
CSF2.0	PR.DS-01
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(d)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO-27001-2022	A.5.33
ITSG-33	IA-5(1)
ITSG-33	SC-28
ITSG-33	SC-28a.
ITSG-33	SC-28(1)
LEVEL	1A
NESA	T5.2.3
PCI-DSSV3.2.1	3.4
PCI-DSSV4.0	3.3.2
PCI-DSSV4.0	3.5.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: (?i)^\h*password\h+([\^# \r]+)\h+pam_unix\.so\h+([\^# \r]+\h+)?use_authtok\b file: /etc/pam.d/
common-password regex: (?i)^\h*password\h+([\^# \r]+)\h+pam_unix\.so\h+([\^# \r]+\h+)?use_authtok\b

Hosts

192.168.40.171

```
Compliant file(s):  
  /etc/pam.d/common-password - regex '(?i)^\h*password\h+([\^#\n\r]+)\h+pam_unix\.so\h+([\^#\n\r]+  
\h+)?use_authtok\b' found - expect '(?i)^\h*password\h+([\^#\n\r]+)\h+pam_unix\.so\h+([\^#\n\r]+\h+)?  
use_authtok\b' found in the following lines:  
    28: password[success=1 default=ignore]pam_unix.so obscure yescrypt use_authtok
```

5.4.1.1 Ensure password expiration is configured

Info

The PASS_MAX_DAYS parameter in /etc/login.defs allows an administrator to force passwords to expire once they reach a defined age.

PASS_MAX_DAYS

<N>

- The maximum number of days a password may be used. If the password is older than this, a password change will be forced. If not specified, -1 will be assumed (which disables the restriction).

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.

We recommend a yearly password change. This is primarily because for all their good intentions users will share credentials across accounts. Therefore, even if a breach is publicly identified, the user may not see this notification, or forget they have an account on that site. This could leave a shared credential vulnerable indefinitely. Having an organizational policy of a 1-year (annual) password expiration is a reasonable compromise to mitigate this with minimal user burden.

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>
```

Edit /etc/login.defs and set PASS_MAX_DAYS to a value greater than 0 that follows local site policy:

Example:

PASS_MAX_DAYS 365

Run the following command to modify user parameters for all users with a password set to a maximum age no greater than 365 or less than 1 that follows local site policy:

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

Example:

```
# awk -F: '($2~/^$.+$/){if($5 > 365 || $5 < 1)system ("chage --maxdays 365 " $1)}/etc/shadow
```

Warning: If a password has been set at system install or kickstart, the last change date field is not set, In this case, setting PASS_MAX_DAYS will immediately expire the password. One possible solution is to populate the last change date field through a command like: `chage -d "$(date +%Y-%m-%d)" root`

Impact:

The password expiration must be greater than the minimum days between password changes or users will be unable to change their password.

Excessive password expiration requirements do more harm than good, because these requirements make users select predictable passwords, composed of sequential words and numbers that are closely related to each other. In these cases, the next password can be predicted based on the previous one (incrementing a number used in the password for example). Also, password expiration requirements offer no containment benefits because attackers will often use credentials as soon as they compromise them. Instead, immediate password changes should be based on key events including, but not limited to:

- Indication of compromise
- Change of user roles
- When a user leaves the organization.

Not only does changing passwords every few weeks or months frustrate the user, but it's also been suggested that it does more harm than good, because it could lead to bad practices by the user such as adding a character to the end of their existing password.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - login.defs - PASSWORD_MAX_DAYS

Compliant file(s):

```
/etc/login.defs - regex '(?i)^\h*PASS_MAX_DAYS\h+\d+\b' found - expect '(?i)^\h*PASS_MAX_DAYS  
\h+365\b' found in the following lines:  
165: PASS_MAX_DAYS365
```

PASSED - shadow password max days

The command '/bin/awk -F: '(\$2~/^\\$.+\\$/) {if(\$5 > 365 || \$5 < 1)print "User: " \$1 " PASS_MAX_DAYS:
" \$5}' /etc/shadow | /bin/awk '{print} END {if (NR == 0) print "pass"; else print "fail"}}'

returned :

pass

5.4.1.3 Ensure password expiration warning days is configured

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.

PASS_WARN_AGE

<N>

- The number of days warning given before a password expires. A zero means warning is given only upon the day of expiration, a negative value means no warning is given. If not specified, no warning will be provided.

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

Edit /etc/login.defs and set PASS_WARN_AGE to a value of 7 or more that follows local site policy:

Example:

PASS_WARN_AGE 7

Run the following command to modify user parameters for all users with a password set to a minimum warning to 7 or more days that follows local site policy:

```
# chage --warndays <N> <user>
```

Example:

```
# awk -F: '($2~/^$.+$/){if($6 < 7)system("chage --warndays 7 " $1)}' /etc/shadow
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.1
800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171	3.13.1
800-171	3.13.2
800-171R3	03.04.01
800-171R3	03.04.02
800-171R3	03.04.06

800-171R3	03.16.01
800-53	CM-2
800-53	CM-6
800-53	CM-7
800-53	CM-7(1)
800-53	CM-9
800-53	SA-3
800-53	SA-8
800-53	SA-10
800-53R5	CM-1
800-53R5	CM-2
800-53R5	CM-6
800-53R5	CM-7
800-53R5	CM-7(1)
800-53R5	CM-9
800-53R5	SA-3
800-53R5	SA-8
800-53R5	SA-10
CSCV7	4.4
CSCV8	4.1
CSF	DE.AE-1
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	ID.AM-08
CSF2.0	ID.IM-01
CSF2.0	ID.IM-02
CSF2.0	ID.IM-03
CSF2.0	ID.RA-09
CSF2.0	PR.DS-10
CSF2.0	PR.IR-03
CSF2.0	PR.PS-01
CSF2.0	PR.PS-06
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.2
ISO-27001-2022	A.5.8
ISO-27001-2022	A.8.9
ISO-27001-2022	A.8.25
ISO-27001-2022	A.8.26

ISO-27001-2022	A.8.27
ISO-27001-2022	A.8.28
ISO-27001-2022	A.8.30
ISO-27001-2022	A.8.31
ISO-27001-2022	A.8.32
ITSG-33	CM-2
ITSG-33	CM-6
ITSG-33	CM-7
ITSG-33	CM-7(1)
ITSG-33	CM-9
ITSG-33	SA-3
ITSG-33	SA-8
ITSG-33	SA-8a.
ITSG-33	SA-10
LEVEL	1A
NESA	T1.2.1
NESA	T1.2.2
NESA	T3.2.5
NESA	T3.4.1
NESA	T4.5.3
NESA	T4.5.4
NESA	T7.2.1
NESA	T7.5.1
NESA	T7.5.3
NESA	T7.6.1
NESA	T7.6.2
NESA	T7.6.3
NESA	T7.6.5
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
PCI-DSSV3.2.1	2.2.2
QCSC-V1	3.2
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - shadow password warn days

The command '/bin/awk -F: '(\$2~/^\$\\$.+\\$/) {if(\$6 < 7)print "User: " \$1 " PASS_WARN_AGE: " \$6}' /etc/shadow | /bin/awk '{print} END {if (NR == 0) print "pass"; else print "fail"}' returned :

pass

PASSED - login.defs - PASS_WARN_AGE

Compliant file(s):

/etc/login.defs - regex '(?i)^\h*PASS_WARN_AGE\h+\d+\b' found - expect '(?i)^\h*PASS_WARN_AGE\h+7\b' found in the following lines:
167: PASS_WARN_AGE7

5.4.1.4 Ensure strong password hashing algorithm is configured

Info

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.

ENCRYPT_METHOD (string) - This defines the system default encryption algorithm for encrypting passwords (if no algorithm are specified on the command line). It can take one of these values:

- MD5 - MD5-based algorithm will be used for encrypting password
- SHA256 - SHA256-based algorithm will be used for encrypting password
- SHA512 - SHA512-based algorithm will be used for encrypting password
- BCRYPT - BCRYPT-based algorithm will be used for encrypting password
- YESCRYPT - YESCRYPT-based algorithm will be used for encrypting password
- DES - DES-based algorithm will be used for encrypting password (default)

Note:

- This parameter overrides the deprecated MD5_CRYPT_ENAB variable.
- This parameter will only affect the generation of group passwords.
- The generation of user passwords is done by PAM and subject to the PAM configuration.
- It is recommended to set this variable consistently with the PAM configuration.

The SHA-512 and yescrypt algorithms provide a stronger hash than other algorithms used by Linux for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local group passwords.

Solution

Edit /etc/login.defs and set the ENCRYPT_METHOD to SHA512 or YESCRYPT :

```
ENCRYPT_METHOD <HASHING_ALGORITHM>
```

Example:

```
ENCRYPT_METHOD YESCRYPT
```

Note:

- This only effects local groups' passwords created after updating the file to use sha512 or yescrypt
- If it is determined that the password algorithm being used is not sha512 or yescrypt once it is changed, it is recommended that all group passwords be updated to use the stronger hashing algorithm.
- It is recommended that the chosen hashing algorithm is consistent across /etc/login.defs and the PAM configuration

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171	3.13.16
800-171R3	03.05.07
800-171R3	03.13.08
800-53	IA-5(1)
800-53	SC-28
800-53	SC-28(1)
800-53R5	IA-5(1)
800-53R5	SC-28
800-53R5	SC-28(1)
CN-L3	8.1.4.7(b)
CN-L3	8.1.4.8(b)
CSCV7	16.4
CSCV8	3.11
CSF	PR.AC-1
CSF	PR.DS-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
CSF2.0	PR.DS-01
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(d)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO-27001-2022	A.5.33
ITSG-33	IA-5(1)
ITSG-33	SC-28
ITSG-33	SC-28a.
ITSG-33	SC-28(1)
LEVEL	1A
NESA	T5.2.3
PCI-DSSV3.2.1	3.4
PCI-DSSV4.0	3.3.2
PCI-DSSV4.0	3.5.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2

SWIFT-CSCV1	4.1
TBA-FIISB	28.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

expect: ^\s*ENCRYPT_METHOD\s+(?i)(SHA512|YESCRYPT)(?-i)\s*\$ file: /etc/login.defs regex: ^\s*ENCRYPT_METHOD\s+

Hosts

192.168.40.171

```
Compliant file(s):
  /etc/login.defs - regex '^\s*ENCRYPT_METHOD\s+' found - expect '^\s*ENCRYPT_METHOD\s+(?i)
(SHA512|YESCRYPT)(?-i)\s*$' found in the following lines:
    284: ENCRYPT_METHOD SHA512
```


5.4.1.5 Ensure inactive password lock is configured

Info

User accounts that have been inactive for over a given period of time can be automatically disabled.

INACTIVE - Defines the number of days after the password exceeded its maximum age where the user is expected to replace this password.

The value is stored in the shadow password file. An input of 0 will disable an expired password with no delay. An input of -1 will blank the respective field in the shadow password file.

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 45 days or less that meets local site policy:

```
# useradd -D -f <N>
```

Example:

```
# useradd -D -f 45
```

Run the following command to modify user parameters for all users with a password set to a inactive age of 45 days or less that follows local site policy:

```
# chage --inactive <N> <user>
```

Example:

```
# awk -F: '($2~/^$.+$/){if($7 > 45 || $7 < 0)system ("chage --inactive 45 " $1)}' /etc/shadow
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

```
-----
PASSED - shadow password inactive days
The command '/bin/awk -F: '($2~/^\$.+\$/ ) {if($7 > 45 || $7 < 0)print "User: " $1 " INACTIVE: " $7}' /etc/shadow | /bin/awk '{print} END {if (NR == 0) print "pass"; else print "fail"}''
returned :

pass

-----
PASSED - useradd - INACTIVE
The command '/sbin/useradd -D | /bin/grep 'INACTIVE'' returned :

INACTIVE=45
```

5.4.1.6 Ensure all users last password change date is in the past

Info

All users should have a password change date in the past.

If a user's 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/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?:i)^\s**\s*\s*pass:?\s**\s*\$

Hosts

192.168.40.171

The command script with multiple lines returned :

Pass

5.4.2.1 Ensure root is the only UID 0 account

Info

Any account with UID 0 has superuser privileges on the system.

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

Run the following command to change the root account UID to 0 :

```
# usermod -u 0 root
```

Modify any users other than root with UID 0 and assign them a new UID.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.5
800-171R3	03.01.06a.
800-53	AC-6(5)
800-53R5	AC-6(5)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.9.2.3
ITSG-33	AC-6(5)
LEVEL	1A
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.6.1
NIAV2	AM32
NIAV2	AM33
NIAV2	VL3a

PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
SWIFT-CSCV1	1.2
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

name: passwd_zero_uid

Hosts

192.168.40.171

No issues found.

5.4.2.2 Ensure root is the only GID 0 account

Info

The usermod command can be used to specify which group the root account belongs to. This affects permissions of files that are created by the root account.

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's GID to 0 :

```
# usermod -g 0 root
```

Run the following command to set the root group's GID to 0 :

```
# groupmod -g 0 root
```

Remove any users other than the root user with GID 0 or assign them a new GID if appropriate.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s**\s**pass:?\s***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- * Correctly configured * :
  - No unauthorized user's GID is: "0"
  - User "root" GID is correctly set to: "0"
```

5.4.2.3 Ensure group root is the only GID 0 group

Info

The groupmod command can be used to specify which group the root group belongs to. This affects permissions of files that are group owned by the root group.

Using GID 0 for the root group helps prevent root group owned files from accidentally becoming accessible to non-privileged users.

Solution

Run the following command to set the root group's GID to 0 :

```
# groupmod -g 0 root
```

Remove any groups other than the root group with GID 0 or assign them a new GID if appropriate.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)

CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

name: group_zero_gid

Hosts

192.168.40.171

No issues found.

5.4.2.4 Ensure root account access is controlled

Info

There are a number of methods to access the root account directly. Without a password set any user would be able to gain access and thus control over the entire system.

Access to root should be secured at all times.

Solution

Run the following command to set a password for the root user:

```
# passwd root
```

- OR -

Run the following command to lock the root user account:

```
# usermod -L root
```

Impact:

If there are any automated processes that relies on access to the root account without authentication, they will fail after remediation.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5

800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2

NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/passwd -S root | /bin/awk '\$2 ~ /^(P|L)/ {print "User: \"\" \$1 \"\" Password is status: \" \$2}'
 expect: (?i)^User: "root" Password is status: (P|L)\$

Hosts

192.168.40.171

The command '/bin/passwd -S root | /bin/awk '\$2 ~ /^(P|L)/ {print "User: \"\" \$1 \"\" Password is status: \" \$2}' returned :

```
User: "root" Password is status: P
```


5.4.2.5 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.

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:

- Locations that are not directories
- Empty directories (::)
- Trailing (:)
- Current working directory ()
- Non root owned directories
- Directories that less restrictive than mode 0755

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.7
800-171R3	03.04.06
800-53	CM-7(2)
800-53R5	CM-7(2)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7(2)
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
QCSC-V1	3.2
SWIFT-CSCV1	2.3

Audit File

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?!)[\s]***[\s]*pass:[\s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  *** PASS ***
- Root's path is correctly configured
```

5.4.2.7 Ensure system accounts do not have a valid login shell

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. Furthermore, a user may add special accounts that are not intended to provide an interactive shell.

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 following command to set the shell for any service accounts returned by the audit to nologin :

```
# usermod -s $(command -v nologin) <user>
```

Example script:

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

{ |_valid_shells="$( awk -F/ '$NF != "nologin" {print}' /etc/shells | sed -rn '/^/{s,/\\V,g;p}' | paste -s -d '|' - )}$"

awk -v pat="$|_valid_shells" -F: '($1!~/^(root|halt|sync|shutdown|nfsnobody)$/ && ($3<"$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)" || $3 == 65534) && $(NF) ~ pat) {system ("usermod -s "$(command -v nologin)" " $1)}/etc/passwd }
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6

800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2

ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^pass\$

Hosts

192.168.40.171

The command script with multiple lines returned :

pass

5.4.2.8 Ensure accounts without a valid login shell are locked

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. Furthermore, a user may add special accounts that are not intended to provide an interactive shell.

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 following command to lock any non-root accounts without a valid login shell returned by the audit:

```
# usermod -L <user>

Example script:

:

#!/usr/bin/env bash

{ I_valid_shells="$(awk -F/ '$NF != "nologin" {print}' /etc/shells | sed -rn '/^/{s,/,\V,g;p}' | paste -s -d '|' -))$"
while IFS= read -r I_user; do passwd -S "$I_user" | awk '$2 !~ /^L/ {system("usermod -L " $1)}'
done < <(awk -v pat="$I_valid_shells" -F: '($1 != "root" && $(NF) !~ pat) {print $1}' /etc/passwd) }
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5

800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6

ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^pass\$

Hosts

192.168.40.171

The command script with multiple lines returned :

pass

5.4.3.2 Ensure default user shell timeout is configured

Info

TMOUT is an environmental setting that determines the timeout of a shell in seconds.

- TMOUT=

n

- Sets the shell timeout to

n

seconds. A setting of TMOUT=0 disables timeout.

- readonly TMOUT- Sets the TMOUT environmental variable as readonly, preventing unwanted modification during run-time.

- export TMOUT - exports the TMOUT variable

System Wide Shell Configuration Files:

- /etc/profile - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in thebash_profile however this file is used to set an initial PATH or PS1 for all shell users of the system. is only executed for interactive

login

shells, or shells executed with the --login parameter.

- /etc/profile.d - /etc/profile will execute the scripts within /etc/profile.d/*.sh It is recommended to place your configuration in a shell script within /etc/profile.d to set your own system wide environmental variables.

- /etc/bashrc - System wide version ofbashrc In Fedora derived distributions, /etc/bashrc also invokes /etc/profile.d/*.sh if

non-login

shell, but redirects output to /dev/null if

non-interactive.

Is only executed for

interactive

shells or if BASH_ENV is set to /etc/bashrc

Setting a timeout value reduces the window of opportunity for unauthorized user access to another user's shell session that has been left unattended. It also ends the inactive session and releases the resources associated with that session.

Solution

Review /etc/bashrc /etc/profile and all files ending in *.sh in the /etc/profile.d/ directory and remove or edit all TMOUT=_n_ entries to follow local site policy. TMOUT should not exceed 900 or be equal to 0

Configure TMOUT in one of the following files:

- A file in the /etc/profile.d/ directory ending insh
- /etc/profile
- /etc/bashrc

TMOUT configuration examples:

- As multiple lines:

TMOUT=900 readonly TMOUT export TMOUT

- As a single line:

readonly TMOUT=900 ; export TMOUT

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.10
800-171	3.1.11
800-171R3	03.01.01h.
800-171R3	03.01.10
800-171R3	03.01.11
800-53	AC-2(5)
800-53	AC-11
800-53	AC-11(1)
800-53	AC-12
800-53R5	AC-2(5)
800-53R5	AC-11
800-53R5	AC-11(1)
800-53R5	AC-12
CN-L3	7.1.2.2(d)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.7(b)
CN-L3	8.1.4.1(b)
CSCV7	16.11
CSCV8	4.3
CSF	PR.AC-1
CSF	PR.AC-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03

CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18
ISO-27001-2022	A.7.7
ISO-27001-2022	A.8.1
ISO-27001-2022	A.8.2
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2(5)
ITSG-33	AC-11
ITSG-33	AC-11(1)
ITSG-33	AC-12
LEVEL	1A
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	NS5j
NIAV2	NS49
NIAV2	SS14e
PCI-DSSV3.2.1	8.1.8
PCI-DSSV4.0	8.2.8
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
TBA-FIISB	36.2.1
TBA-FIISB	37.1.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***[s]*passed:?[s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

grep: : No such file or directory

grep: : No such file or directory

PASSED

TMOUT is configured in: "/etc/profile"

6.1.1.1 Ensure journald service is enabled and active

Info

Ensure that the systemd-journald service is enabled to allow capturing of logging events.

If the systemd-journald service is not enabled to start on boot, the system will not capture logging events.

Solution

Run the following commands to unmask and start systemd-journald.service

```
# systemctl unmask systemd-journald.service # systemctl start systemd-journald.service
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09

CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

```
PASSED - journald active
The command '/bin/systemctl is-active systemd-journald.service' returned :

active

-----
PASSED - journald check - enabled
The command '/bin/systemctl is-enabled systemd-journald.service' returned :

static
```

6.1.1.2 Ensure journald log file access is configured

Info

Journald will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

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

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

If the default configuration is not appropriate for the site specific requirements, copy `/usr/lib/tmpfiles.d/systemd.conf` to `/etc/tmpfiles.d/systemd.conf` and modify as required. Recommended mode for logfiles is 0640 or more restrictive.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)

CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1M
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2

NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?!)[\s]***[\s]*pass:[\s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- File: "/usr/lib/tmpfiles.d/systemd.conf" sets:
  - Directory "/run/user" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/run/systemd/ask-password" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/run/systemd/seats" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/run/systemd/sessions" access is:
```

```
mode: "0755", owned by: "root", and group owned by: "root"
- Directory "/run/systemd/users" access is:
  mode: "0755", owned by: "root", and group owned by: "root"
- Directory "/run/systemd/machines" access is:
  mode: "0755", owned by: "root", and group owned by: "root"
- Directory "/run/systemd/shutdown" access is:
  mode: "0755", owned by: "root", and group owned by: "root"
- Directory "/run/log" access is:
  mode: "0755", owned by: "root", and group owned by: "root"
- Directory "/var/lib/systemd" access is:
  mode: "0755", owned by: "root", and group owned by: "root"
- Directory "/var/lib/systemd/coredump" access is:
  mode: "0755", owned by: "root", and group owned by: "root"
- Directory "/var/lib/systemd/ephemeral-trees" access is:
  mode: "0755", owned by: "root", and group owned by: "root"
- Directory "/var/lib/private" access is:
  mode: "0700", owned by: "root", and group owned by: "root"
- Directory "/var/log/private" access is:
  mode: "0700", owned by: "root", and group owned by: "root"
- Directory "/var/cache/private" access is:
  mode: "0700", owned by: "root", and group owned by: "root"
```

6.1.1.3 Ensure journald log file rotation is configured

Info

Journald includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file `/etc/systemd/journal.conf` is the configuration file used to specify how logs generated by Journald should be rotated.

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.

Solution

Edit `/etc/systemd/journal.conf` or a file ending in `conf` in the `/etc/systemd/journal.conf.d/` directory. Set the following parameters in the `[Journal]` section to ensure logs are rotated according to site policy. The settings should be carefully understood as there are specific edge cases and prioritization of parameters.

Example Configuration

:

```
[Journal] SystemMaxUse=1G SystemKeepFree=500M RuntimeMaxUse=200M RuntimeKeepFree=50M
MaxFileSec=1month
```

Example script to create systemd drop-in configuration file:

```
{ a_settings=("SystemMaxUse=1G" "SystemKeepFree=500M" "RuntimeMaxUse=200M"
"RuntimeKeepFree=50M" "MaxFileSec=1month") [ ! -d /etc/systemd/journal.conf.d/ ] && mkdir /etc/
systemd/journal.conf.d/ if grep -Psq -- '^h*[Journal]' /etc/systemd/journal.conf.d/60-journal.conf;
then printf '%s ' "" "${a_settings[@]}" >> /etc/systemd/journal.conf.d/60-journal.conf else printf '%s ' ""
"[Journal]" "${a_settings[@]}" >> /etc/systemd/journal.conf.d/60-journal.conf fi }
```

Note:

- If these settings appear in a canonically later file, or later in the same file, the setting will be overwritten
- Logfile size and configuration to move logfiles to a remote log server should be accounted for when configuring these settings

Run to following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01

800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1M
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8

PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s**\s**pass:?\s***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
  - Parameter: "SystemMaxUse"
    set to: "1G"
    in the file: "/etc/systemd/journald.conf"
  - Parameter: "SystemKeepFree"
    set to: "100M"
    in the file: "/etc/systemd/journald.conf"
  - Parameter: "RuntimeMaxUse"
    set to: "500M"
    in the file: "/etc/systemd/journald.conf"
  - Parameter: "RuntimeKeepFree"
    set to: "50M"
    in the file: "/etc/systemd/journald.conf"
  - Parameter: "MaxFileSec"
    set to: "1month"
    in the file: "/etc/systemd/journald.conf"
```


6.1.1.4 Ensure only one logging system is in use

Info

Best practices recommend that a single centralized logging system be used for log management, choose a single service either rsyslog - OR - journald to be used as a single centralized logging system.

Configuring only one logging service either rsyslog - OR - journald avoids redundancy, optimizes resources, simplifies configuration and management, and ensures consistency.

Solution

- Determine whether to use journald - OR - rsyslog depending on site needs
- Configure systemd-journald.service
- Configure only ONE either journald - OR - rsyslog and complete the recommendations in that subsection
- Return to this recommendation to ensure only one logging system is in use

Impact:

Transitioning from one logging service to another can be complex and time consuming, it involves reconfiguration and may result in data loss if not managed and reconfigured correctly.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.01
800-53	AU-2
800-53R5	AU-2
CN-L3	8.1.4.3(a)
CSF	PR.PT-1
CSF2.0	PR.PS-04
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a

NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***[s]*pass:?[s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **

- rsyslog is in use
- follow the recommendations in Configure rsyslog subsection only
```

6.1.2.1.1 Ensure systemd-journal-remote is installed

Info

Journald systemd-journal-remote supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralized log management.

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.

Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

Solution

Run the following command to install systemd-journal-remote :

```
# apt install systemd-journal-remote
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1

CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s systemd-journal-remote 2>&1 | /bin/grep -E '(Status:|not installed)'
 expect: ^Status: install ok

Hosts

192.168.40.171

```
The command '/bin/dpkg -s systemd-journal-remote 2>&1 | /bin/grep -E '(Status:|not installed)''  
returned :
```

```
Status: install ok installed
```

6.1.2.1.2 Ensure systemd-journal-upload authentication is configured

Info

Journald systemd-journal-upload supports the ability to send log events it gathers to a remote log host.

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.

Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

Solution

Edit the /etc/systemd/journal-upload.conf file or a file in /etc/systemd/journal-upload.conf.d ending inconf and ensure the following lines are set in the [Upload] section per your environment:

Example settings:

```
[Upload] URL=192.168.50.42 ServerKeyFile=/etc/ssl/private/journal-upload.pem ServerCertificateFile=/etc/ssl/certs/journal-upload.pem TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Example script to create systemd drop-in configuration file:

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

{ a_settings=("URL=192.168.50.42" "ServerKeyFile=/etc/ssl/private/journal-upload.pem"
"ServerCertificateFile=/etc/ssl/certs/journal-upload.pem" "TrustedCertificateFile=/etc/ssl/ca/trusted.pem")
[ ! -d /etc/systemd/journal-upload.conf.d/ ] && mkdir /etc/systemd/journal-upload.conf.d/ if grep -
Psq -- '^h*[Upload]' /etc/systemd/journal-upload.conf.d/60-journald_upload.conf; then printf '%s ' ""
"${a_settings[@]}" ">> /etc/systemd/journal-upload.conf.d/60-journald_upload.conf else printf '%s ' ""
"[journal]" "${a_settings[@]}" ">> /etc/systemd/journal-upload.conf.d/60-journald_upload.conf fi }
```

Run the following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journal-upload
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-2
800-53	AU-7

800-53	AU-12
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1M
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s***\s**pass:?\s***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
  - Parameter: "URL"
    set to: "http://mfdev.aliceblueonline.com:19532"
    in the file: "/etc/systemd/journal-upload.conf.d/10-upload.conf"
  - Parameter: "ServerKeyFile"
    set to: "/etc/ssl/certs/journal.key"
    in the file: "/etc/systemd/journal-upload.conf.d/10-upload.conf"
  - Parameter: "ServerCertificateFile"
    set to: "/etc/ssl/certs/journal.pem"
    in the file: "/etc/systemd/journal-upload.conf.d/10-upload.conf"
  - Parameter: "TrustedCertificateFile"
    set to: "/etc/ssl/certs/journal.crt"
    in the file: "/etc/systemd/journal-upload.conf.d/10-upload.conf"
```


6.1.2.1.3 Ensure systemd-journal-upload is enabled and active

Info

Journald systemd-journal-upload supports the ability to send log events it gathers to a remote log host.

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.

Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

Solution

Run the following commands to unmask, enable and start systemd-journal-upload :

```
# systemctl unmask systemd-journal-upload.service # systemctl --now enable systemd-journal-upload.service
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1

CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

6.1.2.1.3 Ensure systemd-journal-upload is enabled and active

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - journald enabled

The command '/bin/systemctl is-enabled systemd-journal-upload.service' returned :

enabled

PASSED - journald active

The command '/bin/systemctl is-active systemd-journal-upload.service' returned :

active

6.1.2.1.4 Ensure systemd-journal-remote service is not in use

Info

Journald systemd-journal-remote supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

Note:

- The same package, systemd-journal-remote is used for both sending logs to remote hosts and receiving incoming logs.
- With regards to receiving logs, there are two services; systemd-journal-remote.socket and systemd-journal-remote.service

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside it's operational boundary.

Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

Solution

Run the following commands to stop and mask systemd-journal-remote.socket and systemd-journal-remote.service:

```
# systemctl stop systemd-journal-remote.socket systemd-journal-remote.service # systemctl mask systemd-journal-remote.socket systemd-journal-remote.service
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09

CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

```
-----
PASSED - journald remote active
The command '/bin/systemctl is-active systemd-journal-remote.socket systemd-journal-remote.service
| /bin/grep -P -- '^active' | /bin/awk '{print} END {if(NR==0) print "pass"}' returned :

pass

-----
PASSED - journald remote enabled
The command '/bin/systemctl is-enabled systemd-journal-remote.socket systemd-journal-remote.service
| /bin/grep -P -- '^enabled' | /bin/awk '{print} END {if(NR==0) print "pass"}' returned :

pass
```

6.1.2.3 Ensure journald Compress is configured

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.

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

Solution

- IF - rsyslog is the preferred method for capturing logs, this section and Recommendation should be skipped and the "Configure rsyslog" section followed.

- IF - journald is the preferred method for capturing logs:

Set the following parameter in the [Journal] section in /etc/systemd/journald.conf or a file in /etc/systemd/journald.conf.d/ ending inconf :

Compress=yes

Example script to create systemd drop-in configuration file:

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

```
{ a_settings=("Compress=yes") [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir /etc/systemd/journald.conf.d/
if grep -Psq -- '^h*[Journal]' /etc/systemd/journald.conf.d/60-journald.conf; then printf '%s ' ""
"${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf else printf '%s ' "" "[Journal]"
"${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf fi }
```

Note: If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run to following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.06a.

800-53	AU-2
800-53	AU-4
800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-4
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV7	6.4
CSCV8	8.2
CSCV8	8.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.DS-4
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.6
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-4
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NESA	T3.3.1
NESA	T3.6.2
NIAV2	AM7

NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***[s]*pass:?\[s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- Parameter: "Compress"
  correctly set to: "yes"
  in the file: "/etc/systemd/journald.conf"
```


6.1.2.4 Ensure journald Storage is configured

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 due to a reboot.

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.

Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

Solution

- IF - rsyslog is the preferred method for capturing logs, this section and Recommendation should be skipped and the "Configure rsyslog" section followed.

- IF - journald is the preferred method for capturing logs:

Set the following parameter in the [Journal] section in /etc/systemd/journald.conf or a file in /etc/systemd/journald.conf.d/ ending inconf :

Storage=persistent

Example script to create systemd drop-in configuration file:

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

```
{ a_settings=("Storage=persistent") [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir /etc/systemd/journald.conf.d/ if grep -Psq -- '^h*[Journal]' /etc/systemd/journald.conf.d/60-journald.conf; then printf '%s ' "" "${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf else printf '%s ' "" "[Journal]" "${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf fi }
```

Note: If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run to following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01
800-171R3	03.03.03

800-171R3	03.03.06a.
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1

QCSC-V1	3.2
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?!)[\s]***[\s]*pass:[\s]***\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- Parameter: "Storage"
  correctly set to: "persistent"
  in the file: "/etc/systemd/journald.conf"
```

6.1.3.1 Ensure rsyslog is installed

Info

The rsyslog software is recommended in environments where journald does not meet operation requirements.

The security enhancements of rsyslog such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

Solution

Run the following command to install rsyslog :

```
# apt install rsyslog
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01

CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/dpkg -s rsyslog 2>&1 | /bin/grep -E '^(Status: | not installed)'
 expect: ^Status: install ok

Hosts

192.168.40.171

```
The command '/bin/dpkg -s rsyslog 2>&1 | /bin/grep -E '^(Status:|not installed)'' returned :  
Status: install ok installed
```

6.1.3.2 Ensure rsyslog service is enabled and active

Info

Once the rsyslog package is installed, ensure that the service is enabled.

If the rsyslog service is not enabled to start on boot, the system will not capture logging events.

Solution

- IF - rsyslog is being used for logging on the system:

Run the following commands to unmask, enable, and start rsyslog.service :

```
# systemctl unmask rsyslog.service # systemctl enable rsyslog.service # systemctl start rsyslog.service
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03

CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:


```
-----  
PASSED - enabled  
The command '/bin/systemctl is-enabled rsyslog' returned :  
  
enabled  
  
-----  
PASSED - active  
The command '/bin/systemctl is-active rsyslog' returned :  
  
active
```

6.1.3.3 Ensure journald is configured to send logs to rsyslog

Info

Data from systemd-journald may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of systemd-journald logs, however, use of the rsyslog service provides a consistent means of log collection and export.

- IF - rsyslog is the preferred method for capturing logs, all logs of the system should be sent to it for further processing.

Note: This recommendation only applies if rsyslog is the chosen method for client side logging Do not apply this recommendation if systemd-journald is used.

Solution

- IF - Journald is the preferred method for capturing logs, this section and Recommendation should be skipped and the "Configure Journald" section followed.

- IF - rsyslog is the preferred method for capturing logs:

Set the following parameter in the [Journal] section in /etc/systemd/journald.conf or a file in /etc/systemd/journald.conf.d/ ending inconf :

ForwardToSyslog=yes

Example script to create systemd drop-in configuration file:

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

```
{ a_settings=("ForwardToSyslog=yes") [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir /etc/systemd/journald.conf.d/ if grep -Psq -- '^h*[Journal]' /etc/systemd/journald.conf.d/60-journald.conf; then printf '%s ' "${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf else printf '%s ' "" "[Journal]" "${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf fi }
```

Note: If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run to following command to update the parameters in the service:

Restart systemd-journald.service :

```
# systemctl reload-or-restart systemd-journald.service
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.5
800-171	3.3.6

800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.05c.
800-171R3	03.03.06a.
800-53	AU-2
800-53	AU-6(3)
800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-6(3)
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	7.1.3.3(d)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV7	6.5
CSCV8	8.2
CSCV8	8.9
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	DE.DP-4
CSF	PR.PT-1
CSF	RS.AN-1
CSF	RS.AN-3
CSF	RS.CO-2
CSF2.0	DE.AE-02
CSF2.0	DE.AE-03
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.25

ISO-27001-2022	A.6.8
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-6(3)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
NESA	M1.2.2
NESA	M5.2.5
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	5.2.3
QCSC-V1	6.2
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_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

```
-----
PASSED - Ensure ForwardToSyslog set to yes
The command script with multiple lines returned :

- Audit Result:
```

**** PASS ****

- Parameter: "ForwardToSyslog"
correctly set to: "yes"
in the file: "/usr/lib/systemd/journald.conf.d/syslog.conf"

PASSED - systemd-journald.service

The command '/bin/systemctl list-units --type service | grep -P -- '(journald|rsyslog)'' returned :

rsyslog.service	loaded
active running System Logging Service	
systemd-journald.service	loaded
active running Journal Service	

PASSED - rsyslog.service

The command '/bin/systemctl list-units --type service | grep -P -- '(journald|rsyslog)'' returned :

rsyslog.service	loaded
active running System Logging Service	
systemd-journald.service	loaded
active running Journal Service	

6.1.3.4 Ensure rsyslog log file creation mode is configured

Info

rsyslog will create logfiles that do not already exist on the system.

The global() configuration object umask available in rsyslog 8.26.0+, sets the rsyslogd process' umask. If not specified, the system-provided default is used. The value given must always be a 4-digit octal number, with the initial digit being zero.

The legacy \$umask parameter sets the rsyslogd process' umask. If not specified, the system-provided default is used. The value given must always be a 4-digit octal number, with the initial digit being zero.

The legacy \$FileCreateMode parameter allows the setting of the mode with which rsyslogd creates new files. If not specified, the value 0644 is used. The value given must always be a 4-digit octal number, with the initial digit being zero. Please note that the actual permission depend on rsyslogd process umask. If in doubt, use \$umask 0000 right at the beginning of the configuration file to remove any restrictions.

The legacy \$FileCreateMode may be specified multiple times. If so, it specifies the creation mode for all selector lines that follow until the next \$FileCreateMode parameter. Order of lines is vitally important.

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

Solution

Edit either /etc/rsyslog.conf or a dedicated conf file in /etc/rsyslog.d/ and set \$FileCreateMode to 0640 or more restrictive:

```
$FileCreateMode 0640
```

Example script to create a drop-in configuration file in the default include location:

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

```
{ [ ! -d "/etc/rsyslog.d/" ] && mkdir /etc/rsyslog.d/ printf '%s ' "" "$FileCreateMode 0640" >> /etc/rsyslog.d/60-rsyslog.conf }
```

Reload the service:

```
# systemctl reload-or-restart rsyslog
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.3.1

800-171	3.3.2
800-171	3.3.6
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.06a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
800-53R5	MP-2
CN-L3	7.1.2.3(c)
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.3(a)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	5.1
CSCV7	6.2
CSCV7	6.3
CSCV8	3.3
CSCV8	8.2
CSF	DE.CM-1

CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-1
CSF	PR.PT-2
CSF	PR.PT-3
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
ITSG-33	MP-2

ITSG-33	MP-2a.
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1

SWIFT-CSCV1	6.4
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s**\s**pass:?\s**\s*\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
- Parameter: "$FileCreateMode" is correctly set to mode: " "
  in the file: "/etc/rsyslog.conf"
  Should be mode: "640" or more restrictive
```

6.3.1 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.

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.

Run the following commands to initialize AIDE:

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.01
800-171R3	03.03.03
800-53	AC-6(9)
800-53	AU-2
800-53	AU-12
800-53R5	AC-6(9)
800-53R5	AU-2
800-53R5	AU-12
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSCV7	14.9

CSCV8	3.14
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-2
ITSG-33	AU-12
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	7.1.2

PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

```
-----
PASSED - dpkg check aide-common
The command '/bin/dpkg -s aide-common 2>&1 | /bin/grep -E '(Status:|not installed)'' returned :

Status: install ok installed

-----
PASSED - dpkg check aide
The command '/bin/dpkg -s aide 2>&1 | /bin/grep -E '(Status:|not installed)'' returned :

Status: install ok installed
```

6.3.2 Ensure filesystem integrity is regularly checked

Info

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

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

Solution

Run the following command to unmask `dailyaidecheck.timer` and `dailyaidecheck.service` :

```
# systemctl unmask dailyaidecheck.timer dailyaidecheck.service
```

Run the following command to enable and start `dailyaidecheck.timer` :

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

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.02a.
800-171R3	03.03.02b.
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-3
800-53	AU-3(1)
800-53	AU-7
800-53	AU-12
800-53R5	AU-3
800-53R5	AU-3(1)
800-53R5	AU-7
800-53R5	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.2.3(c)
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	8.1.4.3(b)

CSCV7	14.9
CSCV8	8.5
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
ITSG-33	AU-3(1)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1A
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	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - dailyaidecheck.timer enabled
The command '/bin/systemctl list-unit-files | /bin/awk ' \$1~/^dailyaidecheck\.(timer|service)\$/{print \$1 "\t" \$2}'' returned :

dailyaidecheck.servicestatic
dailyaidecheck.timerenabled

PASSED - dailyaidecheck.service static
The command '/bin/systemctl list-unit-files | /bin/awk ' \$1~/^dailyaidecheck\.(timer|service)\$/{print \$1 "\t" \$2}'' returned :

dailyaidecheck.servicestatic
dailyaidecheck.timerenabled

PASSED - aidecheck active
The command '/bin/systemctl is-active dailyaidecheck.timer' returned :

active

7.1.1 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.

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 commands to remove excess permissions, set owner, and set group on /etc/passwd :

```
# chmod u-x,go-wx /etc/passwd # chown root:root /etc/passwd
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)

CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/passwd group: root mask: 133 owner: root

Hosts

192.168.40.171

```
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
```

7.1.2 Ensure permissions on /etc/passwd- are configured

Info

The /etc/passwd- file contains backup user account information.

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 commands to remove excess permissions, set owner, and set group on /etc/passwd- :

```
# chmod u-x,go-wx /etc/passwd- # chown root:root /etc/passwd-
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)

CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/passwd- group: root mask: 133 owner: root

Hosts

192.168.40.171

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-

7.1.3 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.

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 commands to remove excess permissions, set owner, and set group on /etc/group :

```
# chmod u-x,go-wx /etc/group # chown root:root /etc/group
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)

CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/group group: root mask: 133 owner: root

Hosts

192.168.40.171

```
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
```

7.1.4 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.

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 commands to remove excess permissions, set owner, and set group on /etc/group- :

```
# chmod u-x,go-wx /etc/group- # chown root:root /etc/group-
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)

CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/group- group: root mask: 133 owner: root

Hosts

192.168.40.171

```
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-
```

7.1.5 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.

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 one of the following commands to set ownership of /etc/shadow to root and group to either root or shadow :

```
# chown root:shadow /etc/shadow
```

```
-OR- # chown root:root /etc/shadow
```

Run the following command to remove excess permissions form /etc/shadow :

```
# chmod u-x,g-wx,o-rwx /etc/shadow
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2

CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1

NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/shadow group: shadow mask: 137 owner: root

Hosts

192.168.40.171

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

7.1.6 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.

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 one of the following commands to set ownership of /etc/shadow- to root and group to either root or shadow :

```
# chown root:shadow /etc/shadow-  
-OR- # chown root:root /etc/shadow-
```

Run the following command to remove excess permissions form /etc/shadow- :

```
# chmod u-x,g-wx,o-rwx /etc/shadow-
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2

CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1

NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/shadow- group: shadow group: root mask: 137 owner: root

Hosts

192.168.40.171

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-

7.1.7 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.

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 one of the following commands to set ownership of /etc/gshadow to root and group to either root or shadow :

```
# chown root:shadow /etc/gshadow  
-OR- # chown root:root /etc/gshadow
```

Run the following command to remove excess permissions form /etc/gshadow :

```
# chmod u-x,g-wx,o-rwx /etc/gshadow
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2

CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1

NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/gshadow group: root group: shadow mask: 137 owner: root

Hosts

192.168.40.171

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

7.1.8 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.

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 one of the following commands to set ownership of /etc/gshadow- to root and group to either root or shadow :

```
# chown root:shadow /etc/gshadow-  
-OR- # chown root:root /etc/gshadow-
```

Run the following command to remove excess permissions form /etc/gshadow- :

```
# chmod u-x,g-wx,o-rwx /etc/gshadow-
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2

CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1

NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/gshadow- group: root group: shadow mask: 137 owner: root

Hosts

192.168.40.171

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-

7.1.9 Ensure permissions on /etc/shells are configured

Info

/etc/shells is a text file which contains the full pathnames of valid login shells. This file is consulted by chsh and available to be queried by other programs.

It is critical to ensure that the /etc/shells file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run the following commands to remove excess permissions, set owner, and set group on /etc/shells :

```
# chmod u-x,go-wx /etc/shells # chown root:root /etc/shells
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)

CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

file: /etc/shells group: root mask: 133 owner: root

Hosts

192.168.40.171

```
The file /etc/shells with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
permissions : FALSE is compliant with the policy value
```

```
/etc/shells
```

7.1.10 Ensure permissions on /etc/security/opasswd are configured

Info

/etc/security/opasswd and its backup /etc/security/opasswd.old hold user's previous passwords if pam_unix or pam_pwhistory is in use on the system

It is critical to ensure that /etc/security/opasswd is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run the following commands to remove excess permissions, set owner, and set group on /etc/security/opasswd and /etc/security/opasswd.old if they exist:

```
# [ -e "/etc/security/opasswd" ] && chmod u-x,go-rwx /etc/security/opasswd # [ -e "/etc/security/opasswd" ]  
&& chown root:root /etc/security/opasswd # [ -e "/etc/security/opasswd.old" ] && chmod u-x,go-rwx /etc/  
security/opasswd.old # [ -e "/etc/security/opasswd.old" ] && chown root:root /etc/security/opasswd.old
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)

CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1

NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

All of the following must pass to satisfy this requirement:

PASSED - /etc/security/opasswd file permissions

The file /etc/security/opasswd with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven permissions : FALSE is compliant with the policy value

/etc/security/opasswd

PASSED - /etc/security/opasswd.old file permissions

```
The file /etc/security/opasswd.old with fmode owner: root group: root mode: 0600 uid: 0 gid: 0  
uneven permissions : FALSE is compliant with the policy value
```

```
/etc/security/opasswd.old
```

7.2.1 Ensure accounts in /etc/passwd use shadowed passwords

Info

Local accounts can use shadowed passwords. With shadowed passwords, the passwords are saved in the shadow password file, /etc/shadow, encrypted by a salted one-way hash. Accounts with a shadowed password have an x in the second field in /etc/passwd.

The /etc/passwd file also contains information like user ID's and group ID's that are used by many system programs. Therefore, the /etc/passwd file must remain world-readable. In spite of encoding the password with a randomly-generated one-way hash function, an attacker could still break the system if they got access to the /etc/passwd file. This can be mitigated by using shadowed passwords, thus moving the passwords in the /etc/passwd file to /etc/shadow. The /etc/shadow file is set so only root will be able to read and write. This helps mitigate the risk of an attacker gaining access to the encoded passwords with which to perform a dictionary attack.

Note:

- All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.
- A user account with an empty second field in /etc/passwd allows the account to be logged into by providing only the username.

Solution

Run the following command to set accounts to use shadowed passwords and migrate passwords in /etc/passwd to /etc/shadow :

```
# pwconv
```

Investigate to determine if the account is logged in and what it is being used for, to determine if it needs to be forced off.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.2
800-171	3.13.16
800-171R3	03.05.07
800-171R3	03.13.08
800-53	IA-5(1)
800-53	SC-28
800-53	SC-28(1)
800-53R5	IA-5(1)
800-53R5	SC-28
800-53R5	SC-28(1)

CN-L3	8.1.4.7(b)
CN-L3	8.1.4.8(b)
CSCV7	16.4
CSCV8	3.11
CSF	PR.AC-1
CSF	PR.DS-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
CSF2.0	PR.DS-01
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(d)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO-27001-2022	A.5.33
ITSG-33	IA-5(1)
ITSG-33	SC-28
ITSG-33	SC-28a.
ITSG-33	SC-28(1)
LEVEL	1A
NESA	T5.2.3
PCI-DSSV3.2.1	3.4
PCI-DSSV4.0	3.3.2
PCI-DSSV4.0	3.5.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1
TBA-FIISB	28.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

```
cmd: /bin/awk -F: '($2 != "x" ) { print $1 " is not set to shadowed passwords "}' /etc/passwd | /bin/awk
'{print} END {if (NR == 0) print "none"}'
```

expect: ^none\$

Hosts

192.168.40.171

```
The command '/bin/awk -F: '($2 != "x" ) { print $1 " is not set to shadowed passwords "}' /etc/passwd | /bin/awk '{print} END {if (NR == 0) print "none"}' returned :
```

```
none
```

7.2.2 Ensure /etc/shadow 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.

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/benchmarks/18959>

References

800-171	3.5.2
800-171R3	03.05.07
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/awk -F : '(\$2 == "") { print \$1 " does not have a password."}' /etc/shadow | /bin/awk '{print} END {if (NR == 0) print "none"}'

expect: ^none\$

Hosts

192.168.40.171

```
The command '/bin/awk -F : '($2 == "") { print $1 " does not have a password."}' /etc/shadow | /bin/awk '{print} END {if (NR == 0) print "none"}'' returned :
```

```
none
```

7.2.3 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

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/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.01
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-2
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	AT-2
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.2(g)

CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV8	3.3
CSCV8	14.6
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	PR.AA-01
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-2
ITSG-33	AC-3

ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS13c
NIAV2	SS14e
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

name: passwd_invalid_gid

Hosts

192.168.40.171

No issues found.

7.2.4 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.

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

Run the following command to remove all users from the shadow group

```
# sed -ri 's/(^shadow:[^:]*:[^:]*)([^:]+$)/1/' /etc/group
```

Change the primary group of any users with shadow as their primary group.

```
# usermod -g <primary group> <user>
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /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\$

Hosts

192.168.40.171

```
The command '/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
```

7.2.5 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.

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/benchmarks/18959>

References

800-171	3.5.5
800-171	3.5.6
800-171R3	03.05.05c.
800-53	IA-4d.
800-53R5	IA-4d.
CN-L3	8.1.4.1(a)
CSF	PR.AC-1
CSF2.0	PR.AA-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ITSG-33	IA-4d.
LEVEL	1A
NESA	T5.5.2
NIAV2	AM14a
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	5

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

name: passwd_duplicate_uid

Hosts

192.168.40.171

No duplicate User IDs detected

7.2.6 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.

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.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.5.5
800-171	3.5.6
800-171R3	03.05.05c.
800-53	IA-4d.
800-53R5	IA-4d.
CN-L3	8.1.4.1(a)
CSF	PR.AC-1
CSF2.0	PR.AA-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ITSG-33	IA-4d.
LEVEL	1A
NESA	T5.5.2
NIAV2	AM14a
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	5

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

name: group_duplicate_gid

Hosts

192.168.40.171

No duplicate Group IDs detected

7.2.7 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.

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/benchmarks/18959>

References

800-171	3.5.5
800-171	3.5.6
800-171R3	03.05.05c.
800-53	IA-4d.
800-53R5	IA-4d.
CN-L3	8.1.4.1(a)
CSF	PR.AC-1
CSF2.0	PR.AA-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ITSG-33	IA-4d.
LEVEL	1A
NESA	T5.5.2
NIAV2	AM14a
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	5

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

name: passwd_duplicate_username

Hosts

192.168.40.171

No issues found.

7.2.8 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.

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/benchmarks/18959>

References

800-171	3.5.5
800-171	3.5.6
800-171R3	03.05.05c.
800-53	IA-4d.
800-53R5	IA-4d.
CN-L3	8.1.4.1(a)
CSF	PR.AC-1
CSF2.0	PR.AA-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ITSG-33	IA-4d.
LEVEL	1A
NESA	T5.5.2
NIAV2	AM14a
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	5

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

name: group_duplicate_name

Hosts

192.168.40.171

No issues found.

7.2.9 Ensure local interactive user home directories are configured

Info

The user home directory is space defined for the particular user to set local environment variables and to store personal files. While the system administrator can establish secure permissions for users' home directories, the users can easily override these. Users can be defined in `/etc/passwd` without a home directory or with a home directory that does not actually exist.

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory. Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges. If the user's home directory does not exist or is unassigned, the user will be placed in `/` and will not be able to write any files or have local environment variables set.

Solution

If a local interactive users' home directory is undefined and/or doesn't exist, follow local site policy and perform one of the following:

- Lock the user account
- Remove the user from the system
- create a directory for the user. If undefined, edit `/etc/passwd` and add the absolute path to the directory to the last field of the user.

Run the following script to:

- Remove excessive permissions from local interactive users home directories
- Update the home directory's owner

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

```
{ I_output2=""
I_valid_shells="^( $( awk -F/ '$NF != "nologin" {print}' /etc/shells | sed -rn '/^/{s/,\\V,g;p}' | paste -s -d '|' - ) )$"
unset a_uarr && a_uarr=() # Clear and initialize array while read -r I_epu I_eph; do # Populate array with
users and user home location a_uarr+=("$I_epu $I_eph") done <<< "$(awk -v pat="$I_valid_shells" -F: '$(NF) ~
pat { print $1 " " $(NF-1) }' /etc/passwd)"
I_asize="${#a_uarr[@]}" # Here if we want to look at number of users before proceeding [ "$I_asize" -gt
"10000" ] && echo -e "
** INFO **
- \"$I_asize\" Local interactive users found on the system
- This may be a long running process "
while read -r I_user I_home; do if [ -d "$I_home" ]; then I_mask='0027'
I_max="$( printf '%o' $(( 0777 & ~$I_mask )) )"
while read -r I_own I_mode; do if [ "$I_user" != "$I_own" ]; then I_output2="$I_output2
- User: \"$I_user\" Home \"$I_home\" is owned by: \"$I_own\"
- changing ownership to: \"$I_user\"
"
```

```

chown "$l_user" "$l_home"
fi if [ $(( $l_mode & $l_mask )) -gt 0 ]; then l_output2="$l_output2
- User: \"$l_user\" Home \"$l_home\" is mode: \"$l_mode\" should be mode: \"$l_max\" or more restrictive
- removing excess permissions "
chmod g-w,o-rwx "$l_home"
fi done <<< "$(stat -Lc '%U %#a' "$l_home")"
else l_output2="$l_output2
- User: \"$l_user\" Home \"$l_home\" Doesn't exist
- Please create a home in accordance with local site policy"
fi done <<< "$(printf '%s ' "${a_uarr[@]}")"
if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass echo -e " - No modification needed to local
interactive users home directories"
else echo -e "
$l_output2"
fi }

```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)

CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2

NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\s***\s**pass:?\s***\$

Hosts

192.168.40.171

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
- * Correctly configured * :
  - All local interactive users:
    - home directories exist
    - own their home directory
    - home directories are mode: "750" or more restrictive
```

7.2.10 Ensure local interactive user dot files access is configured

Info

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

- forward file specifies an email address to forward the user's mail to.
- rhost file provides the "remote authentication" database for the rcp, rlogin, and rsh commands and the rcmd() function. These files bypass the standard password-based user authentication mechanism. They specify remote hosts and users that are considered trusted (i.e. are allowed to access the local system without supplying a password)
- netrc file contains data for logging into a remote host or passing authentication to an API.
- bash_history file keeps track of the user's commands.

User configuration files with excessive or incorrect access may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

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.

The following script will:

- remove excessive permissions on dot files within interactive users' home directories
- change ownership of dot files within interactive users' home directories to the user
- change group ownership of dot files within interactive users' home directories to the user's primary group
- listforward and rhost files to be investigated and manually deleted

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

```
{ a_output2=(); a_output3=() l_maxsize="1000" # Maximum number of local interactive users before
warning (Default 1,000) l_valid_shells="$( awk -F/ '$NF != "nologin" {print}' /etc/shells | sed -rn '/^/{s,/,\
V,g;p}' | paste -s -d '|' - )}$"
```

```
a_user_and_home=() # Create array with local users and their home directories while read -r l_local_user
l_local_user_home; do # Populate array with users and user home location [[ -n "$l_local_user" ]&& -n
"$l_local_user_home" ]] && a_user_and_home+=("$l_local_user:$l_local_user_home") done <<< "$(awk -v
pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }' /etc/passwd)"
```

```
l_asize="${#a_user_and_home[@]}" # Here if we want to look at number of users before proceeding
[ "${#a_user_and_home[@]}" -gt "$l_maxsize" ] && printf '%s' "" "** INFO **" - "\$l_asize" Local
interactive users found on the system" - "This may be a long running check" ""
```

```
file_access_fix() { a_access_out=() l_max="$( printf '%o' $(( 0777 & ~$l_mask )) )" }
```

```
if [ $(( $l_mode & $l_mask )) -gt 0 ]; then printf '%s' "" - "File: \"$l_hdfilename\" is mode: \"$l_mode\" and should
be mode: \"$l_max\" or more restrictive" " Updating file: \"$l_hdfilename\" to be mode: \"$l_max\" or more
restrictive"
```

```
chmod "$l_change" "$l_hdfilename"
```



```

fi if [[ ! "$l_owner" =~ ($l_user) ]]; then printf '%s ' "" " - File: \"$l_hdfilename\" owned by: \"$l_owner\" and should
be owned by \"${l_user//|/ or}\"" " Updating file: \"$l_hdfilename\" to be owned by \"${l_user//|/ or}\""
chown "$l_user" "$l_hdfilename"

fi if [[ ! "$l_gowner" =~ ($l_group) ]]; then printf '%s ' "" " - File: \"$l_hdfilename\" group owned by: \"$l_gowner\"
and should be group owned by \"${l_group//|/ or}\"" " Updating file: \"$l_hdfilename\" to be group owned by
\"${l_group//|/ or}\""
chgrp "$l_group" "$l_hdfilename"

fi } while IFS= read -r l_user l_home; do a_dot_file=(); a_netrc=(); a_netrc_warn=(); a_bhout=(); a_hdirout=() if
[ -d "$l_home" ]; then l_group="$(id -gn "$l_user" | xargs)"; l_group="$l_group//|/"
while IFS= read -r -d $'0' l_hdfilename; do while read -r l_mode l_owner l_gowner; do case "$(basename
"$l_hdfilename")" in .forward | .rhost ) a_dot_file+=(" - File: \"$l_hdfilename\" exists" " Please review and manually
delete this file") ;;
.netrc ) l_mask='0177'; l_change="u-x,go-rwx"; file_access_fix a_netrc_warn+=(" - File: \"$l_hdfilename\" exists") ;;
.bash_history ) l_mask='0177'; l_change="u-x,go-rwx"; file_access_fix ;;
* ) l_mask='0133'; l_change="u-x,go-wx"; file_access_fix ;;
esac done < <(stat -Lc '%#a %U %G' "$l_hdfilename") done < <(find "$l_home" -xdev -type f -name '.*' -
print0) fi [ "${#a_dot_file[@]}" -gt 0 ] && a_output2+=(" - User: \"$l_user\" Home Directory: \"$l_home\""
"${a_dot_file[@]}") [ "${#a_netrc_warn[@]}" -gt 0 ] && a_output3+=(" - User: \"$l_user\" Home Directory:
\"$l_home\"" "${a_netrc_warn[@]}") done <<< "$(printf '%s ' "${a_user_and_home[@]}")"
[ "${#a_output3[@]}" -gt 0 ] && printf '%s ' "" " ** WARNING **" "${a_output3[@]}" ""
[ "${#a_output2[@]}" -gt 0 ] && printf '%s ' "" "${a_output2[@]}"
}

```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5

800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1A
NESA	T1.3.2

NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^\[s]***[s]*pass:[s]***\$ timeout: 7200

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** PASS **
```

- * Correctly configured * :
- No local interactive users home directories contain:
 - ".forward" or ".rhost" files
 - ".netrc" files with incorrect access configured
 - ".bash_history" files with incorrect access configured
 - ".dot" files with incorrect access configured

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit from CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

PASSED

Hosts

192.168.40.171

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

1.1.1.10 Ensure unused filesystems kernel modules are not available

Info

Filesystem kernel modules are pieces of code that can be dynamically loaded into the Linux kernel to extend its filesystem capabilities, or so-called base kernel, of an operating system. Filesystem kernel modules are typically used to add support for new hardware (as device drivers), or for adding system calls.

While loadable filesystem kernel modules are a convenient method of modifying the running kernel, this can be abused by attackers on a compromised system to prevent detection of their processes or files, allowing them to maintain control over the system. Many rootkits make use of loadable filesystem kernel modules in this way.

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it. The following filesystem kernel modules have known CVE's and should be made unavailable if no dependencies exist:

- afs - CVE-2022-37402
- ceph - CVE-2022-0670
- cifs - CVE-2022-29869
- exfat CVE-2022-29973
- ext CVE-2022-1184
- fat CVE-2022-22043
- fscache CVE-2022-3630
- fuse CVE-2023-0386
- gfs2 CVE-2023-3212
- nfs_common CVE-2023-6660
- nfsd CVE-2022-43945
- smbfs_common CVE-2022-2585

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

- IF - the module is available in the running kernel:
- Unload the filesystem kernel module from the kernel
- Create a file ending inconf with install filesystem kernel modules /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with deny list filesystem kernel modules in the /etc/modprobe.d/ directory

WARNING : unloading, disabling or denylisting filesystem modules that are in use on the system maybe FATAL. It is extremely important to thoroughly review the filesystems returned by the audit before following the remediation procedure.

Example of unloading the gfs2 kernel module:

```
# modprobe -r gfs2 2>/dev/null # rmmod gfs2 2>/dev/null
```

Example of fully disabling the gfs2 kernel module:

```
# printf '%s ' "blacklist gfs2" "install gfs2 /bin/false" >> /etc/modprobe.d/gfs2.conf
```

Note:

- Disabling a kernel module by modifying the command above for each unused filesystem kernel module
- The example gfs2 must be updated with the appropriate module name for the command or example script below to run correctly.

Below is an example Script that can be modified to use on various filesystem kernel modules manual remediation process:

Example Script

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

```
{ a_output2=(); a_output3=(); l_dl="" # Initialize arrays and clear variables l_mod_name="gfs2" # set module
name l_mod_type="fs" # set module type l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type |
sort -u)"

f_module_fix() { l_dl="y" # Set to ignore duplicate checks a_showconfig=() # Create array with modprobe
output while IFS= read -r l_showconfig; do a_showconfig+=("$l_showconfig") done < <(modprobe --
showconfig | grep -P -- 'b(install|blacklist)h+""${l_mod_name//-/}_""b') if lsmod | grep "$l_mod_name"
&& /dev/null; then # Check if the module is currently loaded a_output2+=(" - unloading kernel module:
\"$l_mod_name\") modprobe -r "$l_mod_name" 2>/dev/null; rmmod "$l_mod_name" 2>/dev/null fi
if ! grep -Pq -- 'binstallh+""${l_mod_name//-/}_""h+(/usr)?/bin/(true|false)b' <<< "${a_showconfig[*]}";
then a_output2+=(" - setting kernel module: \"$l_mod_name\" to \"$(readlink -f /bin/false)\"") printf
'%s ' "install $l_mod_name $(readlink -f /bin/false)" >> /etc/modprobe.d/"$l_mod_name".conf fi
if ! grep -Pq -- 'bblacklisth+""${l_mod_name//-/}_""b' <<< "${a_showconfig[*]}"; then a_output2+=("
 - denylisting kernel module: \"$l_mod_name\") printf '%s ' "blacklist $l_mod_name" >> /etc/
modprobe.d/"$l_mod_name".conf fi } for l_mod_base_directory in $l_mod_path; do # Check if the
module exists on the system if [ -d "$l_mod_base_directory/${l_mod_name//-/}" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}")" ]; then a_output3+=(" - \"$l_mod_base_directory\"")
[ [ "$l_mod_name" =~ overlay ] ] && l_mod_name="${l_mod_name::-2}"

[ "$l_dl" != "y" ] && f_module_fix else echo -e " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""

fi done [ "${#a_output3[@]}" -gt 0 ] && printf '%s ' "" -- INFO -- " - module: \"$l_mod_name\" exists in:"
"${a_output3[@]}"

[ "${#a_output2[@]}" -gt 0 ] && printf '%s ' "" "${a_output2[@]}" | | printf '%s ' "" " - No changes needed"
printf '%s ' "" " - remediation of kernel module: \"$l_mod_name\" complete" ""
}
```

Impact:

This list may be quite extensive and covering all edge cases is difficult. Therefore, it's crucial to carefully consider the implications and dependencies before making any changes to the filesystem kernel module configurations.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1M
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Manual Review Required\$

Hosts

192.168.40.171

```
The command script with multiple lines returned :

-- INFO --
The following intentionally skipped
- Kernel module: "xfs"

-- Audit Result: --
** REVIEW the following **
- Kernel module: "ufs" is not fully disabled
- Kernel module: "hpfes" is not fully disabled
- Kernel module: "afs" is not fully disabled <- CVE exists!
- Kernel module: "befes" is not fully disabled
```

```
- Kernel module: "lockd" is not fully disabled
- Kernel module: "coda" is not fully disabled
- Kernel module: "overlay" is not fully disabled
- Kernel module: "efs" is not fully disabled
- Kernel module: "ubifs" is not fully disabled
- Kernel module: "adfs" is not fully disabled
- Kernel module: "orangefs" is not fully disabled
- Kernel module: "zonefs" is not fully disabled
- Kernel module: "dlm" is not fully disabled
- Kernel module: "fuse" is not fully disabled <- CVE exists!
- Kernel module: "f2fs" is not fully disabled
- Kernel module: "exfat" is not fully disabled <- CVE exists!
- Kernel module: "nilfs2" is not fully disabled
- Kernel module: "ceph" is not fully disabled <- CVE exists!
- Kernel module: "autofs" is not fully disabled
- Kernel module: "qnx4" is not fully disabled
- Kernel module: "minix" is not fully disabled
- Kernel module: "netfs" is not fully disabled
- Kernel module: "affs" is not fully disabled
- Kernel module: "smb" is not fully disabled
- Kernel module: "qnx6" is not fully disabled
- Kernel module: "bcache" is not fully disabled
- Kernel module: "pstore" is not fully disabled
- Kernel module: "reiserfs" is not fully disabled
- Kernel module: "9p" is not fully disabled
- Kernel module: "udf" is not fully disabled
- Kernel module: "quota" is not fully disabled
- Kernel module: "gfs2" is not fully disabled <- CVE exists!
- Kernel module: "omfs" is not fully disabled
- Kernel module: "ntfs" is not fully disabled
- Kernel module: "sysv" is not fully disabled
- Kernel module: "bfs" is not fully disabled
- Kernel module [...]
```

1.2.1.1 Ensure GPG keys are configured

Info

Most package managers implement GPG key signing to verify package integrity during installation.

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/benchmarks/18959>

References

800-171	3.11.2
800-171	3.11.3
800-171	3.14.1
800-171R3	03.11.02
800-171R3	03.14.01
800-53	RA-5
800-53	SI-2
800-53	SI-2(2)
800-53R5	RA-5
800-53R5	RA-7
800-53R5	SI-2
800-53R5	SI-2(2)
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
CSCV8	7.3
CSCV8	7.4
CSF	DE.CM-8

CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.IP-12
CSF	RS.CO-3
CSF	RS.MI-3
CSF2.0	GV.SC-10
CSF2.0	ID.IM-01
CSF2.0	ID.IM-02
CSF2.0	ID.IM-03
CSF2.0	ID.RA-01
CSF2.0	ID.RA-08
CSF2.0	PR.PS-02
GDPR	32.1.b
GDPR	32.1.d
HIPAA	164.306(a)(1)
ISO-27001-2022	A.6.8
ISO-27001-2022	A.8.8
ISO-27001-2022	A.8.32
ISO/IEC-27001	A.12.6.1
ITSG-33	RA-5
ITSG-33	SI-2
ITSG-33	SI-2(2)
LEVEL	1M
NESA	M1.2.2
NESA	M5.4.1
NESA	T7.6.2
NESA	T7.7.1
NIAV2	PR9
PCI-DSSV3.2.1	6.1
PCI-DSSV3.2.1	6.2
PCI-DSSV4.0	6.3
PCI-DSSV4.0	6.3.1
PCI-DSSV4.0	6.3.3
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
SWIFT-CSCV1	2.2
SWIFT-CSCV1	2.7

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/apt-key list expect: ^Manual Review Required\$

Hosts

192.168.40.171

The command '/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/ubuntu-keyring-2012-cdimage.gpg

pub rsa4096 2012-05-11 [SC]
 8439 38DF 228D 22F7 B374 2BC0 D94A A3F0 EFE2 1092
uid [unknown] Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.com>

/etc/apt/trusted.gpg.d/ubuntu-keyring-2018-archive.gpg

pub rsa4096 2018-09-17 [SC]
 F6EC B376 2474 EDA9 D21B 7022 8719 20D1 991B C93C
uid [unknown] Ubuntu Archive Automatic Signing Key (2018) <ftpmaster@ubuntu.com>

/etc/apt/trusted.gpg.d/ubuntu-pro-esm-apps.gpg

pub rsa4096 2019-11-21 [SC]
 E8A4 43CE 3581 13D1 87BE E0E6 AB01 A101 DB53 907B
uid [unknown] Ubuntu Apps Automatic Signing Key <esm@canonical.com>
sub rsa4096 2019-11-21 [E]

/etc/apt/trusted.gpg.d/ubuntu-pro-esm-infra.gpg

pub rsa4096 2019-04-17 [SC]
 56F7 650A 24C9 E9EC F87C 4D8D 4067 E403 13CB 4B13
uid [unknown] Ubuntu Extended Security Maintenance Automatic Signing Key v2
 <esm@canonical.com>
sub rsa4096 2019-04-17 [E]

1.2.1.2 Ensure package manager repositories are configured

Info

Systems need to have package manager repositories configured to ensure they receive the latest patches and updates.

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/benchmarks/18959>

References

800-171	3.11.2
800-171	3.11.3
800-171	3.14.1
800-171R3	03.11.02
800-171R3	03.14.01
800-53	RA-5
800-53	SI-2
800-53	SI-2(2)
800-53R5	RA-5
800-53R5	RA-7
800-53R5	SI-2
800-53R5	SI-2(2)
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
CSCV8	7.3
CSCV8	7.4
CSF	DE.CM-8

CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.IP-12
CSF	RS.CO-3
CSF	RS.MI-3
CSF2.0	GV.SC-10
CSF2.0	ID.IM-01
CSF2.0	ID.IM-02
CSF2.0	ID.IM-03
CSF2.0	ID.RA-01
CSF2.0	ID.RA-08
CSF2.0	PR.PS-02
GDPR	32.1.b
GDPR	32.1.d
HIPAA	164.306(a)(1)
ISO-27001-2022	A.6.8
ISO-27001-2022	A.8.8
ISO-27001-2022	A.8.32
ISO/IEC-27001	A.12.6.1
ITSG-33	RA-5
ITSG-33	SI-2
ITSG-33	SI-2(2)
LEVEL	1M
NESA	M1.2.2
NESA	M5.4.1
NESA	T7.6.2
NESA	T7.7.1
NIAV2	PR9
PCI-DSSV3.2.1	6.1
PCI-DSSV3.2.1	6.2
PCI-DSSV4.0	6.3
PCI-DSSV4.0	6.3.1
PCI-DSSV4.0	6.3.3
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
SWIFT-CSCV1	2.2
SWIFT-CSCV1	2.7

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/apt-cache policy expect: ^Manual Review Required\$

Hosts

192.168.40.171

The command '/bin/apt-cache policy' returned :

Package files:

```
100 /var/lib/dpkg/status
   release a=now
500 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages
   release v=24.04,o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=multiverse,b=amd64
   origin security.ubuntu.com
500 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages
   release v=24.04,o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=universe,b=amd64
   origin security.ubuntu.com
500 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages
   release v=24.04,o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=restricted,b=amd64
   origin security.ubuntu.com
500 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages
   release v=24.04,o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=main,b=amd64
   origin security.ubuntu.com
100 http://in.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages
   release v=24.04,o=Ubuntu,a=noble-backports,n=noble,l=Ubuntu,c=universe,b=amd64
   origin in.archive.ubuntu.com
100 http://in.archive.ubuntu.com/ubuntu noble-backports/main amd64 Packages
   release v=24.04,o=Ubuntu,a=noble-backports,n=noble,l=Ubuntu,c=main,b=amd64
   origin in.archive.ubuntu.com
500 http://in.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages
   release v=24.04,o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=multiverse,b=amd64
   origin in.archive.ubuntu.com
500 http://in.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages
   release v=24.04,o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=universe,b=amd64
   origin in.archive.ubuntu.com
500 http://in.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages
   release v=24.04,o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=restricted,b=amd64
   origin in.archive.ubuntu.com
500 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages
   release v=24.04,o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=main,b=amd64
   origin in.archive.ubuntu.co [...]
```


2.1.22 Ensure only approved services are listening on a network interface

Info

A network port is identified by its number, the associated IP address, and the type of the communication protocol such as TCP or UDP.

A listening port is a network port on which an application or process listens on, acting as a communication endpoint.

Each listening port can be open or closed (filtered) using a firewall. In general terms, an open port is a network port that accepts incoming packets from remote locations.

Services listening on the system pose a potential risk as an attack vector. These services should be reviewed, and if not required, the service should be stopped, and the package containing the service should be removed. If required packages have a dependency, the service should be stopped and masked to reduce the attack surface of the system.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Run the following commands to stop the service and remove the package containing the service:

```
# systemctl stop <service_name>.socket <service_name>.service # apt purge <package_name>
```

- OR - If required packages have a dependency:

Run the following commands to stop and mask the service and socket:

```
# systemctl stop <service_name>.socket <service_name>.service # systemctl mask <service_name>.socket <service_name>.service
```

Note: replace <service_name> with the appropriate service name.

Impact:

There may be packages that are dependent on the service's package. If the service's package is removed, these dependent packages will be removed as well. Before removing the service's package, review any dependent packages to determine if they are required on the system.

- IF - a dependent package is required: stop and mask the <service_name>.socket and <service_name>.service leaving the service's package installed.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6

800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1M
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/ss -plntu expect: ^Manual Review Required\$

Hosts

192.168.40.171

The command '/bin/ss -plntu' returned :

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
udp	UNCONN	0	0	127.0.0.54:53	0.0.0.0:*	users:(("systemd-resolve",pid=2084968,fd=16))
udp	UNCONN	0	0	127.0.0.53%lo:53	0.0.0.0:*	users:(("systemd-resolve",pid=2084968,fd=14))

```
udp UNCONN 0 0 192.168.40.171%ens160:68 0.0.0.0:* users:(("systemd-  
network",pid=2084963,fd=22))
```

```
[...]
```

3.1.1 Ensure IPv6 status is identified

Info

Internet Protocol Version 6 (IPv6) is the most recent version of Internet Protocol (IP). It's designed to supply IP addressing and additional security to support the predicted growth of connected devices. IPv6 is based on 128-bit addressing and can support 340 undecillion, which is 340,282,366,920,938,463,374,607,431,768,211,456 unique addresses.

Features of IPv6

- Hierarchical addressing and routing infrastructure
- Statefull and Stateless configuration
- Support for quality of service (QoS)
- An ideal protocol for neighboring node interaction

IETF RFC 4038 recommends that applications are built with an assumption of dual stack. It is recommended that IPv6 be enabled and configured in accordance with Benchmark recommendations.

- IF - dual stack and IPv6 are not used in your environment, IPv6 may be disabled to reduce the attack surface of the system, and recommendations pertaining to IPv6 can be skipped.

Note: It is recommended that IPv6 be enabled and configured unless this is against local site policy

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Enable or disable IPv6 in accordance with system requirements and local site policy

Impact:

IETF RFC 4038 recommends that applications are built with an assumption of dual stack.

When enabled, IPv6 will require additional configuration to reduce risk to the system.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7

800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1M
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: /bin/grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && echo -e "

- IPv6 is enabled " || echo -e "

- IPv6 is not enabled "

expect: Manual Review Required

Hosts

192.168.40.171

```
The command '/bin/grep -Pqs '^h*0\b' /sys/module/ipv6/parameters/disable && echo -e "\n - IPv6 is
enabled\n" || echo -e "\n - IPv6 is not enabled\n"' returned :

- IPv6 is not enabled
```

4.2.5 Ensure ufw outbound connections are configured

Info

Configure the firewall rules for new outbound connections.

Note:

- Changing firewall settings while connected over network can result in being locked out of the system.
- Unlike iptables, when a new outbound rule is added, ufw automatically takes care of associated established connections, so no rules for the latter kind are required.

If rules are not in place for new outbound 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 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
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
800-171R3	03.13.01
800-171R3	03.13.06
800-53	CA-9
800-53	SC-7
800-53	SC-7(5)
800-53R5	CA-9
800-53R5	SC-7
800-53R5	SC-7(5)
CN-L3	7.1.2.2(c)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSCV8	4.4
CSCV8	4.5
CSF	DE.CM-1

CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7
ITSG-33	SC-7(5)
LEVEL	1M
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
NIAV2	GS7b
NIAV2	NS25
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	1.2.1
PCI-DSSV4.0	1.4.1
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
SWIFT-CSCV1	2.1
TBA-FIISB	43.1

Audit File

Policy Value

cmd: /sbin/ufw status numbered expect: ^Manual Review Required\$

Hosts

192.168.40.171

```
The command '/sbin/ufw status numbered' returned :

Status: active

      To      Action      From
      --      -
[ 1] 22/tcp    ALLOW IN    Anywhere
[ 2] 80/tcp    ALLOW IN    Anywhere
[ 3] 443/tcp   ALLOW IN    Anywhere
[ 4] 3306/tcp  ALLOW IN    Anywhere
[ 5] 33060/tcp ALLOW IN    Anywhere
[ 6] 6379/tcp  ALLOW IN    127.0.0.1
[ 7] 8443/tcp  ALLOW IN    Anywhere
[ 8] 8080/tcp  ALLOW IN    Anywhere
[ 9] 19532/tcp ALLOW IN    Anywhere
[10] 8005/tcp  ALLOW IN    Anywhere
[11] 53/udp    ALLOW IN    Anywhere
[12] 68/udp    ALLOW IN    Anywhere
[13] Anywhere on lo    ALLOW IN    Anywhere
[14] Anywhere    ALLOW OUT   Anywhere on lo    (out)
[15] Anywhere    DENY IN     127.0.0.0/8
[16] Anywhere    ALLOW OUT   Anywhere on all    (out)
[17] 53          ALLOW IN    Anywhere
[18] 8181        ALLOW IN    Anywhere
[19] 8761        ALLOW IN    Anywhere
[20] 25          ALLOW IN    Anywhere
[21] 514/tcp     ALLOW IN    Anywhere
[22] 514/udp     ALLOW IN    Anywhere
[23] 5000        ALLOW IN    Anywhere
```


5.1.6 Ensure sshd Ciphers are configured

Info

This variable limits the ciphers that SSH can use during communication.

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 compliant are:

-

aes256-gcm@openssh.com

-

aes128-gcm@openssh.com

- aes256-ctr

- aes192-ctr

- aes128-ctr

Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised.

- The Triple DES ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain clear text data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack.

- Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plain text data from an arbitrary block of cipher text in an SSH session via unknown vectors.

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 Ciphers line to contain a comma separated list of the site unapproved (weak) Ciphers preceded with a - above any Include entries:

Example:

Ciphers -3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,chacha20-poly1305@openssh.com

- IF - CVE-2023-48795 has been addressed, and it meets local site policy, chacha20-poly1305@openssh.com may be removed from the list of excluded ciphers.

Note: First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

See Also

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
800-171R3	03.05.07
800-171R3	03.05.12
800-171R3	03.13.08
800-53	AC-17(2)
800-53	IA-5
800-53	IA-5(1)
800-53	SC-8
800-53	SC-8(1)
800-53R5	AC-17(2)
800-53R5	IA-5
800-53R5	IA-5(1)
800-53R5	SC-8
800-53R5	SC-8(1)
CN-L3	7.1.2.7(g)
CN-L3	7.1.3.1(d)
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.1(c)
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
CSCV8	3.10
CSF	PR.AC-1
CSF	PR.AC-3
CSF	PR.DS-2
CSF	PR.DS-5
CSF	PR.PT-4
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
CSF2.0	PR.AA-05
CSF2.0	PR.DS-02
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO-27001-2022	A.5.33
ISO-27001-2022	A.6.7
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.2.2
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	AC-17(2)
ITSG-33	IA-5
ITSG-33	IA-5(1)
ITSG-33	SC-8
ITSG-33	SC-8a.
ITSG-33	SC-8(1)
LEVEL	1A
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T5.2.3
NESA	T5.4.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	AM37
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS5d
NIAV2	NS6b
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	3.2

QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	2.1
SWIFT-CSCV1	2.6
SWIFT-CSCV1	4.1
TBA-FIISB	29.1

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Manual Review Required\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
port 22: ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
Pass
```

6.1.3.5 Ensure rsyslog logging is configured

Info

The rsyslog and configuration files specifies rules for logging and which files are to be used to log certain classes of messages.

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.).

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Edit the following lines in the configuration file(s) returned by the audit as appropriate for your environment.

Note: The below configuration is shown for example purposes only. Due care should be given to how the organization wishes to store log data.

```
*.emerg :omusrmsg:* auth,authpriv.* /var/log/secure mail.* -/var/log/mail mail.info -/var/log/mail.info
mail.warning -/var/log/mail.warn mail.err /var/log/mail.err cron.* /var/log/cron
```

```
*.=warning;*.=err -/var/log/warn
```

```
*.crit /var/log/warn
```

```
*.*;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/
log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages
```

Run the following command to reload the rsyslogd configuration:

```
# systemctl reload-or-restart rsyslog
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171R3	03.03.01
800-171R3	03.03.03
800-171R3	03.03.06a.
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53R5	AU-2
800-53R5	AU-7

800-53R5	AU-12
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF	RS.AN-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
CSF2.0	RS.AN-03
CSF2.0	RS.AN-06
CSF2.0	RS.AN-07
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1M
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
QCSC-V1	13.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Manual Review Required\$

Hosts

192.168.40.171

The command script with multiple lines returned :

/etc/rsyslog.d/50-default.conf:auth,authpriv.*	/var/log/auth.log
/etc/rsyslog.d/50-default.conf:*. *;auth,authpriv.none	-/var/log/syslog
/etc/rsyslog.d/50-default.conf:cron.*	/var/log/cron.log
/etc/rsyslog.d/50-default.conf:kern.*	-/var/log/kern.log
/etc/rsyslog.d/50-default.conf:mail.*	-/var/log/mail.log
/etc/rsyslog.d/50-default.conf:*.=warning;*.=err	-/var/log/warn
/etc/rsyslog.d/50-default.conf:*.crit	/var/log/warn
/etc/rsyslog.d/50-default.conf:*. *;mail.none;news.none	-/var/log/messages
/etc/rsyslog.d/50-default.conf:local0,local1.*	-/var/log/localmessages
/etc/rsyslog.d/50-default.conf:local2,local3.*	-/var/log/localmessages
/etc/rsyslog.d/50-default.conf:local4,local5.*	-/var/log/localmessages
/etc/rsyslog.d/50-default.conf:local6,local7.*	-/var/log/localmessages
/etc/rsyslog.d/50-default.conf:mail.info	-/var/log/mail.info
/etc/rsyslog.d/50-default.conf:mail.warn	-/var/log/mail.warn
/etc/rsyslog.d/50-default.conf:mail.err	/var/log/mail.err

6.1.3.7 Ensure rsyslog is not configured to receive logs from a remote client

Info

rsyslog supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside its operational boundary.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Unless the system's primary function is to serve as a logfile server , modify the files returned by the Audit Procedure and remove the specific lines highlighted by the audit. Verify none of the following entries are present in the rsyslog configuration.

advanced format

```
module(load="imtcp") input(type="imtcp" port="514")
```

deprecated legacy format

```
$ModLoad imtcp $InputTCPServerRun
```

Reload the service:

```
# systemctl reload-or-restart rsyslog
```

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.02
800-171R3	03.04.06
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	9.2
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3

CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?:i)^\s***\s**pass:?\s***\\$

Hosts

192.168.40.171

The command script with multiple lines returned :

```
- Audit Result:
  ** FAIL **
  - Reason(s) for audit failure:
  - Advanced format entry to accept incoming logs: "module(load="imtcp")"
    found in: "/etc/rsyslog.d/10-listen.conf"
  - Advanced format entry to accept incoming logs: "input(type="imtcp" port="514" ruleset="discard")"
    found in: "/etc/rsyslog.d/10-listen.conf"
  - Obsolete format entry to accept incoming logs: "module(load="imtcp")"
    found in: "/etc/rsyslog.d/10-listen.conf"
  - Obsolete format entry to accept incoming logs: "input(type="imtcp" port="514" ruleset="discard")"
    found in: "/etc/rsyslog.d/10-listen.conf"
```

6.1.3.8 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

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 provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Edit /etc/logrotate.conf or the appropriate configuration file provided by the script in the Audit Procedure, as necessary to ensure logs are rotated according to site policy.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-53	AU-4
800-53R5	AU-4
CSCV7	6.4
CSCV8	8.3
CSF	PR.DS-4
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.6
ITSG-33	AU-4
LEVEL	1M
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Manual Review Required\$

Hosts

192.168.40.171

```
The command script with multiple lines returned :

# /etc/logrotate.conf
# see "man logrotate" for details

# global options do not affect preceding include directives

# rotate log files weekly
weekly

# use the adm group by default, since this is the owning group
# of /var/log/.
su root adm

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
#dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may also be configured here.

# /etc/logrotate.d/alternatives
/var/log/alternatives.log {
monthly
rotate 12
compress
delaycompress
missingok
notifempty
create 644 root root
}

# /etc/logrotate.d/apt
/var/log/apt/term.log {
rotate 12
monthly
compress
missingok
notifempty
}

/var/log/apt/history.log {
rotate 12
monthly
compress
missingok
```

```

    notifempty
}

# /etc/logrotate.d/bootlog
/var/log/boot.log
{
    missingok
    daily
    copytruncate
    rotate 7
    notifempty
}

# /etc/logrotate.d/btmp
# no packages own btmp -- we'll rotate it here
/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}

# /etc/logrotate.d/cloud-init
/var/log/cloud-init*.log
{
    su root root
    missingok
    nocreate
    notifempty
    rotate 6
    compress
    delaycompress
    size 1M
}

# /etc/logrotate.d/dpkg
/var/log/dpkg.log {
    monthly
    rotate 12
    compress
    delaycompress
    missingok
    notifempty
    create 644 root root
}

# /etc/logrotate.d/falcon-sensor
/var/log/falcon-sensor.log {
    rotate 7
    daily
    sharedscripts
    postrotate
        /usr/bin/pkill -HUP falcon-sensor
    endscript
}

# /etc/logrotate.d/mysql-server
# - I put everything in one block and added sharedscripts, so that mysql gets
#   flush-logs'd only once.
#   Else the binary logs would automatically increase by n times every day.
# - The error log is obsolete, messages go to syslo [...]

```

7.1.13 Ensure SUID and SGID files are reviewed

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 or SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

There are valid reasons for SUID and SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different checksum than what from the package. This is an indication that the binary may have been replaced.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Ensure that no rogue SUID or SGID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

See Also

<https://workbench.cisecurity.org/benchmarks/18959>

References

800-171	3.1.1
800-171	3.1.4
800-171	3.1.5
800-171	3.8.1
800-171	3.8.2
800-171	3.8.3
800-171R3	03.01.02
800-171R3	03.01.04
800-171R3	03.01.05a.
800-171R3	03.08.02
800-53	AC-3
800-53	AC-5
800-53	AC-6
800-53	MP-2
800-53R5	AC-3
800-53R5	AC-5
800-53R5	AC-6
800-53R5	MP-2
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(a)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.3
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.7.7
ISO-27001-2022	A.7.10
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.1.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-5
ITSG-33	AC-6
ITSG-33	MP-2
ITSG-33	MP-2a.
LEVEL	1M
NESA	T1.3.2
NESA	T1.3.3
NESA	T1.4.1
NESA	T4.2.1

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
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	AM1
NIAV2	AM3
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
NIAV2	SS29
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit

Policy Value

name: find_suid_sgid_files

Hosts

192.168.40.171

The following 25 files are SUID or SGID:

```

/usr/lib/snapd/snap-confine
  owner: root, group: root, permissions: 4755

/usr/lib/dbus-1.0/dbus-daemon-launch-helper
  owner: root, group: messagebus, permissions: 4754

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

```

```
owner: root, group: root, permissions: 4755

/usr/lib/openssh/ssh-keysign
owner: root, group: root, permissions: 4755

/usr/lib/x86_64-linux-gnu/utempter/utempter
owner: root, group: utmp, permissions: 2755

/usr/bin/chage
owner: root, group: shadow, permissions: 2755

/usr/bin/sudo
owner: root, group: root, permissions: 4755

/usr/bin/dotlockfile
owner: root, group: mail, permissions: 2755

/usr/bin/chsh
owner: root, group: root, permissions: 4755

/usr/bin/expiry
owner: root, group: shadow, permissions: 2755

/usr/bin/fusermount3
owner: root, group: root, permissions: 4755

/usr/bin/gpasswd
owner: root, group: root, permissions: 4755

/usr/bin/mount
owner: root, group: root, permissions: 4755

/usr/bin/newgrp
owner: root, group: root, permissions: 4755

/usr/bin/su
owner: root, group: root, permissions: 4755

/usr/bin/umount
owner: root, group: root, permissions: 4755

/usr/bin/ssh-agent
owner: root, group: _ssh, permissions: 2755

/usr/bin/crontab
owner: root, group: crontab, permissions: 2755

/usr/bin/passwd
owner: root, group: root, permissions: 4755

/usr/bin/chfn
owner: root, group: root, permissions: 4755

/usr/sbin/unix_chkpwd
owner: root, group: shadow, permissions: 2755

/usr/sbin/pam_extrausers_chkpwd
owner: root, group: shadow, permissions: 2755

/usr/sbin/postqueue
owner: root, group: postdrop, permissions: 2555

/usr/sbin/postdrop
owner: root, group: postdrop, permissions: 2555

/usr/libexec/ssh-keysign
owner: root, group: root, permissions: 4711
```

Remediations

Suggested Remediations